Návrh prvků a úloh laboratoře pro praktickou výuku bezdrátových sítí

Draft elements and exercise of laboratory for practical teaching wireless network

Bc. Miroslav Píša

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

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

Jméno a příjmení:	**Bc. Miroslav PÍŠA**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Návrh prvků a úloh laboratoře pro praktickou výuku bezdrátových sítí**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na dané téma.**
2. **Analyzujte současný stav výuky bezdrátových sítí na FAI.**
3. **Vyberte vhodné HW prvky do laboratoře a navrhněte jejich zapojení.**
4. **Navrhněte a realizujte praktické laboratorní úlohy.**
5. **Vypracujte ukázkové protokoly jednotlivých laboratorních úloh.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BARKEN, Lee. Jak zabezpečit bezdrátovou síť Wi-Fi. Přeložil Jiří Veselský. 1. vyd. Brno: Computer Press, 2004. 176 s. ISBN 80-251-0346-3.**
2. **PUŽMOVÁ, Rita. Bezpečnost bezdrátové komunikace: Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G. 1. vyd. Brno: Computer Press, 2005. 184 s. ISBN 80-251-0791-4.**
3. **ZANDL, Patrick. Bezdrátové sítě Wi-Fi: Praktický průvodce. 1. vyd. Brno: Computer Press, 2003. 204 s. ISBN 80-7226-632-2.**
4. **KÖHRE, Thomas. Stavíme si bezdrátovou síť Wi-fi. Přeložil Marek Šiller. 1. vyd. Brno: Computer Press, 2004. 296 s. ISBN 80-251-0391-9.**
5. **BRISBIN, Shelly. Wi-Fi -- postavte si svou vlastní wi-fi síť. 1. vyd. Praha: Neocortex, 2004. 239 s. ISBN 80-86330-13-3.**
6. **HORÁK, Jaroslav. Malá počítačová síť doma a ve firmě. 1. vyd. Praha: Grada, 2003. 183 s. ISBN 80-24705-82-6.**
7. **TRULOVE, James. Sítě LAN: hardware, instalace a zapojení. Přeložil Tomáš Znamenáček. 1. vyd. Praha: Grada, 2009. 384 s. ISBN 978-80-247-2098-2.**

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

Datum zadání diplomové práce: **19. února 2010**

Termín odevzdání diplomové práce: **8. června 2010**

Ve Zlíně dne 19. února 2010

prof. Ing. Vladimír Vašek, CSc.
děkan

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

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Tato práce se zabývá návrhem prvků a úloh laboratoře pro výuku bezdrátových wifi sítí. Teoretická část obsahuje základní seznámení s problematikou wifi sítí. Praktická část se pak věnuje zhodnocení současného stavu praktické výuky bezdrátových wifi sítí na FAI, UTB ve Zlíně. Návrh jednotlivých hard-warových prvků, jejich popis a zapojení v laboratoři. Dále návrh zadání 10 laboratorních úloh a nakonec popis zkušební realizace celého projektu včetně vypracování příslušných protokolů.

Klíčová slova: bezdrátová síť, wifi, výuka, přístupový bod, autentizace, RADIUS, WEP, WPA

ABSTRACT

This work deals with a design of components and functions of a laboratory for teaching about wireless network. The theoretical part contains elemental introduction to questions about wifi. The practical part contains an evaluation of the contemporary conditions of teaching about wireless network at FAI, UTB in Zlin, the design of single hard-ware parts, their description and connection in laboratory. Then it also contains a concept of 10 laboratory exercises and finally a description of a trial realization of the whole project including elaboration of pertinent exercises.

Keywords: wireless network, wifi, teaching, access point, authentication, RADIUS, WEP, WPA.

Děkuji vedoucímu mojí diplomové práce, Ing. Miroslavu Matýskovi Ph.D, za odborné vedení, cenné rady a připomínky potřebné a přínosné pro vypracování mojí diplomové práce. Můj vděk patří také všem, kteří mi při této práci i studiu podporovali a pomáhali mi.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Výhod které nám počítače nabízejí dnes využívá téměř každý. Navíc se vyskytla nutnost tyto počítače spojovat a tím vytvářet počítačové sítě různých velikostí. Ty jsou v dnešní době nedílnou součástí nejen firem, kanceláří a komerčních institucí ale v stále větší míře se vyskytují i v menším měřítku v domácnostech. Jedná se jak o sítě lokální, tak i o sítě připojené k světové síti internet.

Od doby, kdy byly realizovány první počítačové sítě již uplynulo mnoho let a spolu s těmito lety se vyvíjel způsob jejich metod, jakými byli realizovány. Od prvních metalických sítí realizovaných pomocí sériových a paralelních kabelů se přešlo ke koaxialnímu kabelu a následně pak ke kroucené dvojlince neboli TP kabelu. V posledních několika letech dochází ale také k velkému rozmachu sítí bezdrátových. Ty sebou přinesly větší komfort pro uživatele v podobě osvobození se od kabelu a nutnosti být poblíž síťové zásuvky.

Spolu s pohodlím a mobilitou, které bezdrátová síť představují, představují i veliké riziko z pohledu zabezpečení přenášených dat. Data, která putují takovou sítí nám doslova „létají pod nosem“ a může je zachytit každý, kdo bude v dosahu signálu a kdo k tomu bude mít příslušné vybavení. Otázka bezpečnosti je proto nedílnou součástí budování bezdrátové sítě.V dnešní době však technologie bezdrátových sítí nabízí mnoho způsobů, jak tuto síť efektivně zabezpečit.

Znalost technologie bezdrátových sítí je pro absolventa oboru Informačních technologií nutností jak po stránce teoretické, tak i praktické. Proto se tato práce zabývá návrhem laboratoře, ve které se studenti budou moci seznámit s bezdrátovými síťovími prvky, vyzkoušet si jejich administraci, vytvářet jednoduché bezdrátové sítě a aplikovat na ně základní metody jejich zabezpečení.

I. TEORETICKÁ ČÁST

1 BEZDRÁTOVÁ SÍŤ, WI-FI

Bezdrátové sítě se velice rychle staly součástí života každého z nás. Jako první se objevily sítě pro hlasovou komunikaci, které postupem času vytlačily pevné telefonní přípojky. Tyto mobilní sítě (GSM/GPRS/EDGE a UMTS) ať v jakékoli podobě v dnešní době využívá téměř každý.

Využívání bezdrátové konektivity se stalo natolik oblíbeným, že se velice brzy začaly vyvíjet první specifikace datových bezdrátových sítí, jako náhrada za pevné metalické počítačové sítě. Tak vznikly sítě v lokálním měřítku, WLAN (Wireless Local Area Network), a s nimi nejpopulárnější bezdrátový standard: Wi-Fi(802.11b). Tyto sítě byli v počátku naprosto odlišné od mobilních sítí a nedokázaly s nimi komunikovat. WLAN byli sítě výhradně pro datovou komunikaci, mobilní sítě pro komunikaci hlasovou. WLAN také omezovaly pohyb uživatele na dosah přístupového bodu, oproti tomu sítě mobilní podporovaly plnou mobilitu uživatele.

Bezdrátové sítě jsou pro firmy i domácí uživatele neuvěřitelně atraktivní, protože poskytují značnou míru pružnosti a svobody, která vyplývá ze ztráty závislosti na fyzické kabeláži. Fyzické připojení je klaustrofobií. Bezdrátová technologie naopak nabízí svobodu přesouvat se podle chuti.. Bezdrátové lokální sítě dnes nabízejí kavárny, hotely, letiště a další místa, kde mohou návštěvníci použít své přenosné počítače či PDA (Persondal Digital Assistant), přečíst si poštu či surfovat na internetu [1].

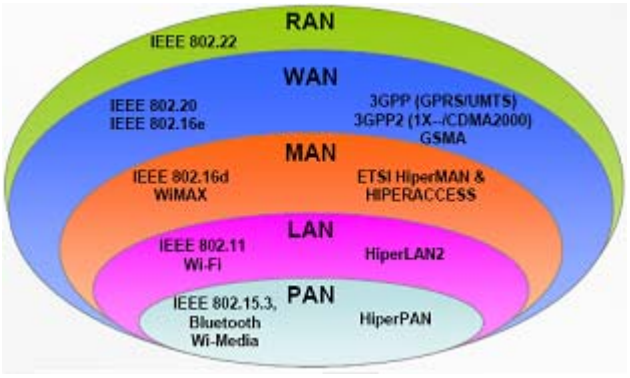
WiFi (Wireless Fidelity) je bezdrátová, síť určená primárně k náhradě kabelového ethernetu v bezlicenčním pásmu, které je dostupné prakticky v celém civilizovaném světě. Hlavní výhodou této technologie je její nízká cena, způsobená mimo jiné tím, že certifikovaná zařízení jsou k dispozici ve velkých sériích. Protože požadavky na certifikaci zařízení jsou běžně dostupné a norma 802.11b dokonce volně k dispozici na webu, existují řádově desítky (možná již stovky) různých výrobců, počínaje NoName přidružená výroba věznice v Šen Čou a konče velkými korporacemi typu CISCO Systems, 3Com nebo Microsoft.
Cena a možnosti jednotlivých zařízení na trhu se přirozeně velmi liší, nicméně jejich interoperabilita je zabezpečena právě logem WiFi [11].

1.1 Standard IEEE 802

IEEE (The Institute of Electrical and Electronics Engineers) je největší profesní a standardizační organizace na světě, založená roku 1884, jejíž aktivity mimo pořádání konferencí a vydávání odborných časopisů zahrnují přípravu a vydávání komunikačních a síťových standardů [7]. IEEE sdružuje přes 350 000 elektroinženýrů a informatiků v cca 150 zemích ve všech světadílech. IEEE vydává více než 100 titulů odborných periodik a řadu knih (25% světové produkce odborné literatury v elektrotechnice a informatice pochází z IEEE), pořádá konference a všemožně podporuje rozvoj oboru [12].

IEEE 802, standardizační výbor zabývající se problematikou lokálních sítí byl vytvořen v roce 1980 a je tvořen několika podvýbory. Bezdrátovou komunikací se zabývají :

- **IEEE 802.11** : Bezdrátové lokální sítě (WLAN, Wireless Local Area Network)
- **IEEE 802.15** : Bezdrátové osobní sítě (WPAN, Wireless Personal Area Network,)
- **IEEE 802.16** : Bezdrátové městské sítě (WMAN, Wireless Metropolitan Area Network)
- **IEEE 802.20** : Širokopásmový mobilní přístup (MBWA, Mobile Broadband Wireless Access, 2002)
- **IEEE 802.22** : Oblastní bezdrátové sítě (WRAN, Wireless Regional Area Network)



Obr. 1. Bezdrátové standardy [14]

1.1.1 IEEE 802.11

Standard IEEE 802.11 byl schválen v roce 1997 jako první světový bezdrátový standard pro lokální sítě. Skupina která se zabývala jeho vývojem byla založena už roku 1990.

Původní specifikace definovala síť v pásmu 2,4 GHz s rychlostmi přenosu 1 a 2 Mbit/s, brzy se však stala nedostačující a tak bylo v rámci tohoto standardu vytvořeno několik podskupin, které tento standard doplňují nebo rozšiřují. Jejich vytváření pokračuje dodnes.

Jednotlivé podskupiny standardu 802.11(v závorce je vždy uveden rok schválení):

- **802.11a** : Bezdrátové sítě pracující na frekvenci 5 GHz, což má za následek zlepšení ze strany interferencí, ovšem slabinou je zpětná kompatibilita se sítěmi 802.11 b a 802.11g. Oproti 802.11b a g má povolen větší vyzařovací výkon, lze jej tudíž použít na větší vzdálenosti. Rychlost přenosu se pohybuje kolem 20 Mbit/s (1999).
- **802.11b** : Tuto specifikaci dnes používá většina Wi-Fi zařízení. Definuje bezdrátové sítě pracující na frekvenci 2,4 GHz s teoretickou přenosovou rychlostí až 11 Mbit/s. Tento podstandard je nejvíce spojován se skratkou Wi-Fi (1999).
- **802.11c** : Definuje práci síťových mostů v bezdrátových sítích. V podstatě jde o doplněk standardu 802.1D (2003).
- **802.11d** : tzv. „*Globální harmonizační standard*“, Definuje požadavky na fyzickou vrstvu k uspokojení regulačních domén nepokrytých existujícími standardy. Liší se v povolených frekvencích, vyzařovacích výkonech a propustnosti signálu. Specifikace eliminuje nutnost vývoje a výroby specifických produktů pro různé země (2001) [15].
- **802.11e** : Doplňuje podporu pro kvalitu služeb (*Quality of Service*, QoS) pro zajištění přenosu hovorového signálu, obrazu apod. IEEE 802.11e doplňuje sítě definované IEEE 802.11a/b/g. Doplněk navíc zajišťuje zpětnou kompatibilitu se zařízeními, které nejsou podporou pro QoS vybaveny (2003) [16].
- **802.11f** : Doplněk IEEE 802.11F vylepšuje mechanismus předávání stanic (*Roaming*) při přechodu mezi dvěma rádiovými kanály nebo z jedné sítě do sousední s připojením k jinému přístupovému bodu. Protokol IAPP (*Inter-Access Point Protocol*) umožňuje spolupráci přístupových bodů od různých výrobců. (2003) [16].
- **802.11g** : Jde o obdobu 802.11a, ovšem je specifikován pro sítě pracující v pásmu 2.4GHz. Maximální přenosová rychlost je zvýšena až na 54Mbit/s. Zajišťuje zpětnou kompatibilitu se standardem 802.11b (2003).

- **802.11h** : Standard rozšiřuje 802.11a o evropské podmínky pro použití bezdrátových sítí v pásmu 5GHz mimo budovy. Zavádí dynamický výběr kanálu (*Dynamic Channel Selection*) a řízení vysílacího výkonu (*Transmit Power Control*) (2003).
- **802.11i** : zlepšuje zabezpečení bezdrátových sítí 802.11 použitím AES (*Advanced Encryption Standard*) šifrování namísto WEPu. Produkty certifikované pro tento standard jsou označeny WPA (Wi-Fi Protected Access) (2004).
- **802.11j** : Doplněk pro použití pásma 4,9 – 5 GHz pro multimediální služby v bezdrátových sítích. Používá se zatím pouze v Japonsku (2004).
- **802.11k** : Doplněk pro zefektivnění využití přenosového média na základě měření kvality jednotlivých kanálů, šumu, zahlcení a vzájemného rušení. Na základě těchto informací dojde k optimalizaci nastavení klientů a ke konfiguraci sítě tak, aby se dospělo k co největší kvalitě spoje (2008) [16].
- **802.11n** : Skupina IEEE 802.11n studuje různé možnosti nastavení parametrů fyzické vrstvy a MAC (Media Access Control) podvrstvy pro zvýšení datové propustnosti. Mezi tyto možnosti patří použití více antén, změny kódovacích schémat a změny MAC protokolů. Aktuální cíl skupiny je přenosová rychlost minimálně 100 Mbit/s nad MAC vrstvou. Navíc má IEEE 802.11n zajistit vyšší dosah se zachováním co největší rychlosti a zvětšit odolnost proti rušení 2009 [16].
- **802.11r** : Specifikace pro rychlé přesuny uživatelů mezi přístupovými body (*2008*).
- **802.11w** : Rozšíření stávající MAC vrstvy o mechanismy na podporu integrity dat, autenticity zdroje dat, utajení dat a ochrany před útoky typu replay pro vybrané rámce určené pro management. Cílem je zvýšení zabezpečení rámců pro management (2009) [16].
- **802.11x** : Neformální obecné označení kteréhokoli z doplňujících standardů 802.11
- **802.11X** : Bezpečnostní standard bezdrátových i metalických sítí založený na autentifikaci a filtrování portů při přístupu k síti. Běžně nesprávně označován jako 802.11x.

Doposud neschválené standardy :

- **802.11.l** : Rezervováno a nebude použito.

- **802.11m** : Kontrola dokumentů vydaných ostatními skupinami a oprava případných nesrovnalostí a chyb v původních specifikacích.
- **802.11o** : Rezervováno a nebude použito.
- **802.11p** : Podpora připojení stanic umístěných v pohyblivých prostředích (auta,vlaky…) k pevným přístupovým bodům.
- **802.11q** : Rezervováno a nebude použito.
- **802.11s** : Standard pro samoorganizující se bezdrátové mesh sítě. Používá tzv. „Multi-hopping“, každý klient je zároveň i přístupovým bodem a naopak.
- **802.11u** : Doplněk organizující spoluprácí se sítěmi mimo standardy 802.
- **802**.**11v** : Vytváří jednotné rozhraní pro management zařízení v bezdrátové síti. Stanice budou moci provádět funkce managementu zahrnující monitoring a konfiguraci buď centralizovaně, nebo distribuovaně prostřednictvím mechanismu na druhé vrstvě [16].

1.2 Frekvenční pásma bezdrátových sítí 802.11

Na rozdíl od řady jiných bezdrátových standardů běží 802.11 na „volné“ části rádiového spektra. To znamená, že pro vysílání a komunikaci není potřeba žádná licence. Volnými částmi rádiového spektra, které využívá 802.11 (a Wi-Fi), jsou pásma 2,4GHz a 5 GHz. Tato volná spektra využívá také mnoho domácích zařízení, jako například mikrovlnné trouby a bezdrátové domácí telefony [8]. Při provozu zařízení v těchto frekvenčních pásmech je třeba pouze dodržovat podmínky stanovené generální licencí GL12/R/200 pro pásmo 2.4 GHz a GL 30/R/200 pro pásmo 5 GHz.

V různých zemích světa se však využívá různý frekvenční rozsah. V některých státech jako např. USA je zakázáno používat určité části frekvenčního spektra z důvodu rušení jiných zařízení pracujících na těchto frekvencích. Česká republika se však drží evropské konvence ETSI která dává k dispozici plné frekvenční spektrum.

1.2.1 Frekvenční pásmo 2,4 GHz

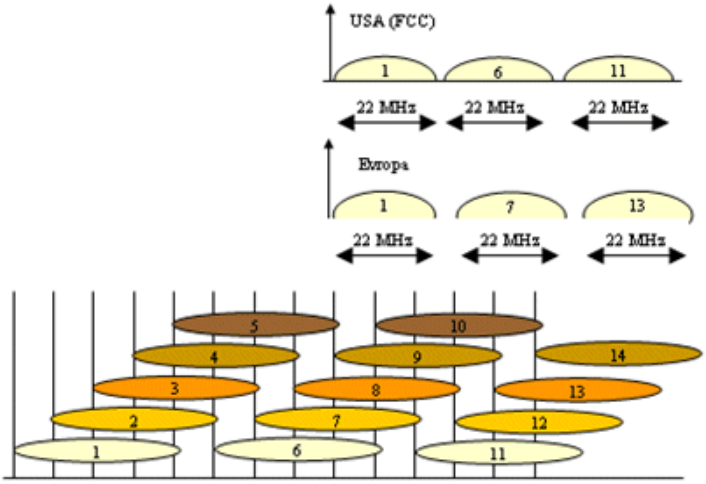
Bezdrátové sítě 802.11b/g pracují v pásmu 2,4 GHz, což ovšem znamená frekvenční rozsah 2,4 GHz až 2,4835 GHz, tedy pásmo široké 83,5 MHz. Jelikož technologie 802.11b

potřebuje ke své činnosti kanál o šířce 22MHz, bez překrývání by se do tohoto rozsahu vešly pouze 3 kanály. V praxi se však používá 14 částečně se překrývajících kanálů. Mezi jednotlivými kanály je odstup 5MHz, přenos na 2 sousedních kanálech je tedy možný, nedosahuje však takových kvalit jako v případě 2 nepřekrývajících se kanálů. V praxi, pokud je to tedy možné, je lepší při budování sítě zvolit kanál, který se co nejméně překrývá se sousedními sítěmi. Následující tabulka (Tab. 1) zobrazuje jednotlivé kanály a jejich použití ve světě.

Tab. 1. Frekvenční rozsahy kanálů a jejich využití v různých zemích

Kanál	Frekvence [GHz]	USA,Kanada	Evropa	Japonsko
1	2401-2423	x	x	x
2	2406-2428	x	x	x
3	2411-2433	x	x	x
4	2416-2438	x	x	x
5	2421-2443	x	x	x
6	2426-2448	x	x	x
7	2431-2453	x	x	x
8	2436-2458	x	x	x
9	2441-2463	x	x	x
10	2446-2468	x	x	x
11	2451-2473	x	x	x
12	2456-2478	---	x	x
13	2461-2483	---	x	x
14	2466-2488	---	---	x

Evropské státy, kromě Francie (10 a 11 kanál) a Španělska (10-13 kanál), se drží konvence ETSI (European Telecommunications Standards Institute), která dovoluje používat plné frekvenční spektrum. V ČR , a ve většině ostatních Evropských zemí, je povoleno vybrat pro provoz bezdrátových sítí 3 vzájemně se nepřekrývající kanály, tedy na kanálech 1, 7 a 13. V USA je situace obdobná, ovšem tam se jedná o kanály 1, 6 a 11. Z následujícího obrázku (Obr. 2) je patrné že v USA jsou mezi sousedními kanály mnohem menší odstupy.



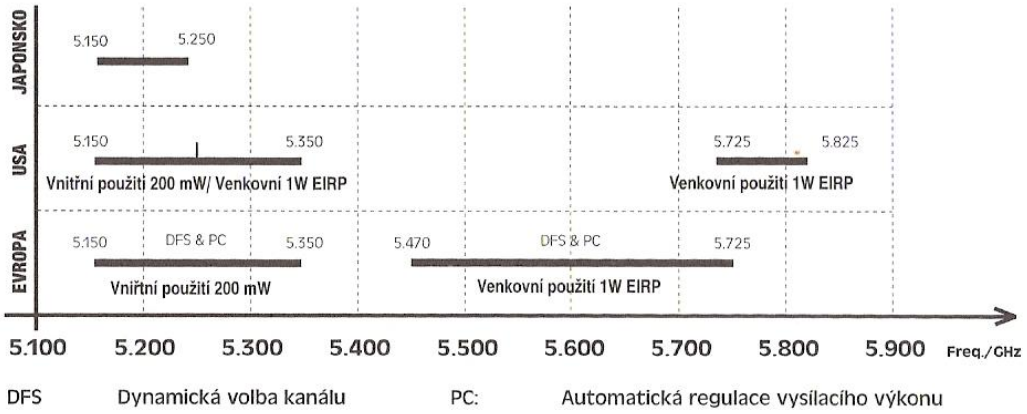
Obr. 2. Frekvenční kanály v pásmu 2,4 GHz [17]

1.2.2 Frekvenční pásmo 5 GHz

Frekvenční pásmo 5 GHz je podstatně širší než 2,4 GHz, zatím však nedošlo ke shodě při jeho uvolňování a využití mezi americkou organizací FCC a evropským regulačním orgánem EU. Původní návrhy na standard 802.11a totiž nebraly v úvahu fakt, že v jiných zemích než je USA se pásmo 5GHz využívá pro jiné účely. Standard 802.11a dělí spektrum podle výstupního výkonu na 3 rozsahy :

- **5,150-5,250 GHz**: použití pouze uvnitř budov, maximální hustota vyzářeného výkonu 23 dBi tj. 200 mW EIRP (Equivalent Isotropically Radiated Power) (přesněji 0.25 MHz/25 MHz v každém 25 MHz úseku)
- **5,250-5,350 GHz** : stejné jako výše, navíc ale je max. hustota výkonu definována jako (10 mW/MHz v libovolném 1 MHz úseku). Zařízení v tomto pásmu navíc musí být vybaveny automatickou regulací výkonu, která může snížit podle podmínek výstupní výkon zařízení na polovinu (-3 dB). Tato regulace ale nemusí být zapnuta, potom ovšem je maximální vyzářený výkon poloviční vždy, tj. 100 mW EIRP. Zařízení se také musí umět automaticky naladit na frekvenci, kde není v provozu radar fungující na stejné frekvenci
- **5,47 - 5,725 GHz** : použití uvnitř i vně budov, maximální vyzářený výkon 1 W EIRP (30 dBi). I zde ale platí podmínka o vybavenosti automatickou regulací

výkonu se stejnými pravidly, tj. není-li regulace zapnuta, je max. vyzářený výkon 0.5W (27 dBi) a podmínka o automatickém přelaďování.Rozdíly ve využití jednotlivých kanálů mezi Evropou, USA a Japonskem jsou vidět na následujícím obrázku (Obr. 3).



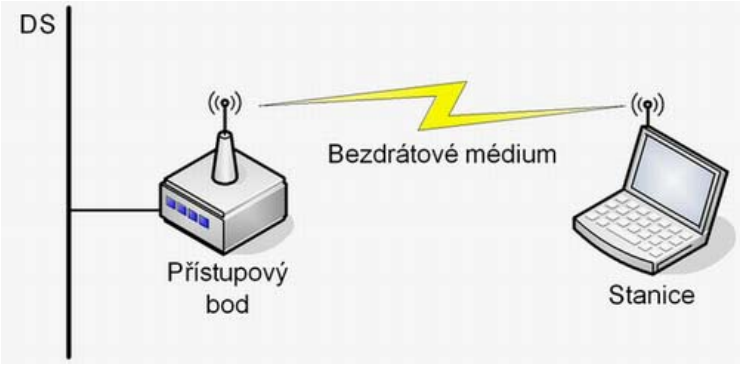
Obr. 3. Využití pásma 5 GHz ve světě [3]

1.3 Komponenty sítě

Každá ze sítí 802.11 obsahuje čtyři hlavní druhy fyzických komponent :

- Distribuční systém
- Přístupový bod (access point, AP)
- Bezdrátové médium
- Stanice

V praxi lze tyto čtyři komponenty shrnout do dvou nebo tří, protože bezdrátové médium je funkcionalitou využívanou stanicí i přístupovým bodem a distribuční systém (kabelová síť) není potřeba v případě, když od bezdrátové sítě neočekáváme propojení do jiné sítě a má sloužit pouze k zajištění komunikace mezi bezdrátově připojenými stanicemi [3].



Obr. 4. Komponenty sítě 802.11

1.3.1 Distribuční systém

Distribuční systém je logickou komponentou bezdrátové sítě. Jakmile je síť tvořena více přístupovými body, je třeba zajistit jejich vzájemnou komunikaci pomocí distribučního systému. Standard 802.11 přímo nespecifikuje, jak má být distribuční systém realizován, určuje pouze jaké má poskytovat funkce.

V naprosté většině komerčních systémů je distribuční systém řešen jako kombinace síťového mostu a distribučního média, jímž je páteřní síť používaná pro přenášení dat mezi přístupovými body [3].

1.3.2 Přístupový bod

Jde o přemostění mezi kabelovou a bezdrátovou sítí a ačkoli poskytuje i celou řadu dalších funkcí, funkce mostu mezi bezdrátovou a kabelovou částí je nejdůležitější [3].

1.3.3 Bezdrátové médium

Bezdrátové médium je pro sítě WLAN tímtéž, co kabeláž pro sítě kabelové. Bezdrátové médium je nosičem dat při přesunu dat od stanice ke stanici. Mohli bychom říci, že tím médiem je vzduch, což je ovšem nesmysl (ostatně sítě WLAN fungují i ve vzduchoprázdnu). Bezdrátovým médiem 802.11 se rozumí dvě radiová frekvenční pásma (2,4 a 5 GHz).

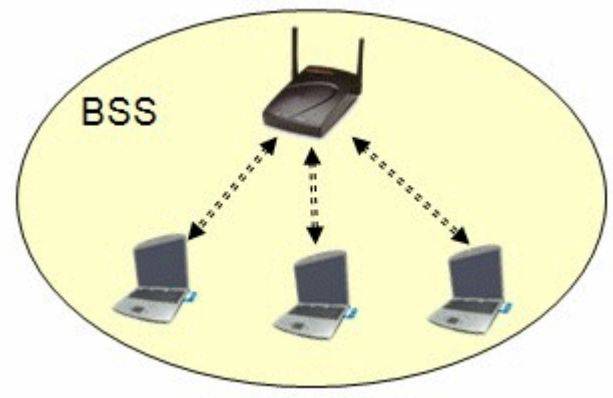
1.3.4 Stanice

Stanicí se v bezdrátové síti rozumí jakékoli zařízení které se dokáže do sítě připojit, Notebook, PDA, počítač. Podmínkou není ani mobilita připojeného zařízení. Příkladem

mohou být firemní bezdrátové sítě tam, kde není možnost instalace síťové kabeláže. V takových případech se nemusí řešit, zda se uživatel do sítě připojuje s notebookem, nebo stolním počítačem, který nikam nepřenáší.

1.4 Architektura WLAN

Základní stavební blok 802.11 sítě označujeme jako Basic Service Set (BSS), tedy základní soubor služeb. Jde o skupinu stanic, které spolu komunikují. Tato společná komunikace probíhá v území vymezeném průnikem dosahu těchto stanic a takovéto území nazýváme Basic Service Area (BSA) [3].



Obr. 5. Basic Service Set (BSS) [17]

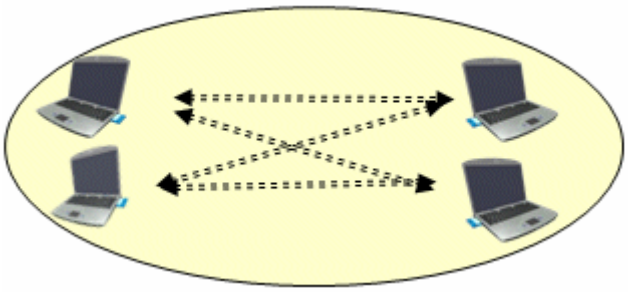
Bezdrátové sítě mohou pracovat ve dvou základních režimech. Je to buď režim IBSS (Independed Basic Service Set), též označovaný jako režim Ad-hoc. V tomto případě se klienti spojují přímo mezi sebou navzájem. Druhým režimem je BSS/ESS (Basic Service Set/Extended Service Set) neboli režim infrastruktury. V těchto sítích se využívá centrálních přístupových bodů (Access Point).

1.4.1 IBSS (Ad-hoc) režim

Sítě Ad-hoc se někdy rovněž nazývají nezávislé sítě, to z toho důvodu, že jednotlivé stanice v takové síti spolu komunikují přímo, podle potřeby, a tedy nezávisle na nějakém prostředníkovi. Z toho vyplývá, že pokud spolu stanice chtějí komunikovat, musí být ve vzájemném rádiovém dosahu. Pro menší síť s několika stanicemi vzdálenými pár metrů od sebe je to vhodné komunikační schéma, ale je zřejmé, že sítě s více počítači, nebo sítě v členitějších a rozlehlejších prostorách, kde princip vzájemného radiového dosahu nemůže být vždy zajištěn, takto realizovat nelze.

Nejčastější použití sítí Ad-hoc je propojení několika počítačů z nějakého specifického důvodu a na omezený čas – kupříkladu LAN party, nárazová výměna dat atd. [3].

Avšak bezpečnostní dopady tohoto uspořádání jsou samozřejmě zcela zásadní. Pro připojení do sítě Ad-hoc stačí znát použitý kanál a SSID. V tomto režimu sice lze použít i WEP, nicméně specifikace WPA už sítě IBSS neošetřuje a jejich zabezpečení tak bude řádně vyřešeno až s příchodem standardu 802.11i [1].

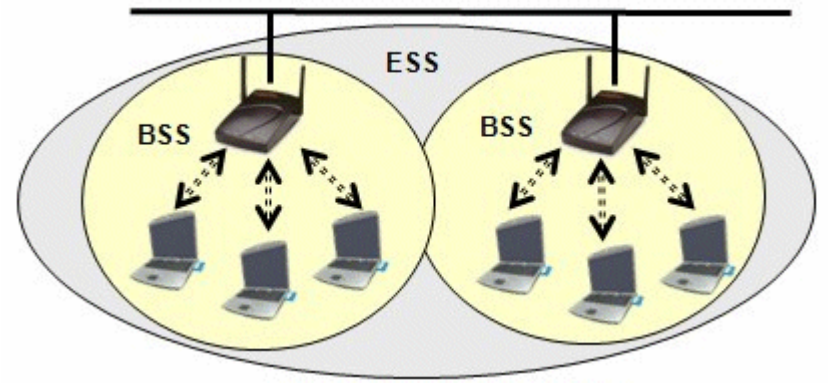


Obr. 6. Síť v režimu IBSS (Ad-hoc) [17]

1.4.2 BSS/ESS režim (sítě s infrastrukturou)

Zkratka BSS označuje AP připojené k metalické infrastruktuře, například Ethernetu. Jednotlivé bezdrátové stanice se připojují k centrálnímu přístupovému bodu a veškerý provoz (dokonce i přímý provoz mezi klienty) se směřuje přes AP.

ESS (Extended Service Set) jsou dvě nebo více BSS, propojené nějakým distribučním systémem, například Ethernetem. Vztah BSS/ESS ukazuje následující obrázek (Obr. 7.).



Obr. 7. Wifi síť ESS složená z buněk BSS [17]

V tomto režimu AP funguje jako most mezi metalickou a bezdrátovou sítí. V závislosti na typu a nastavení se může chovat skutečně jako „hloupý“ most na druhé síťové vrstvě, anebo může fungovat mnohem chytřeji jako směrovač, zajišťovat překlad adres (NAT),

přidělování adres (DHCP) a další. Volba AP tedy v každém případě závisí na tom, jak plánujete infrastrukturu sítě.

V režimu infrastruktury je významným bezpečnostním rizikem neoprávněný přístup ke vzdálené správě AP. Útočník, který získá přístup ke správě zařízení, bude moci zobrazit/změnit klíče protokolů WEP/WAP, bude moci ovlivnit jiná nastavení, což může vést k porušení ochrany dat a k útokům DoS (Denial of Service) [1].

2 ZABEZPEČENÍ WLAN

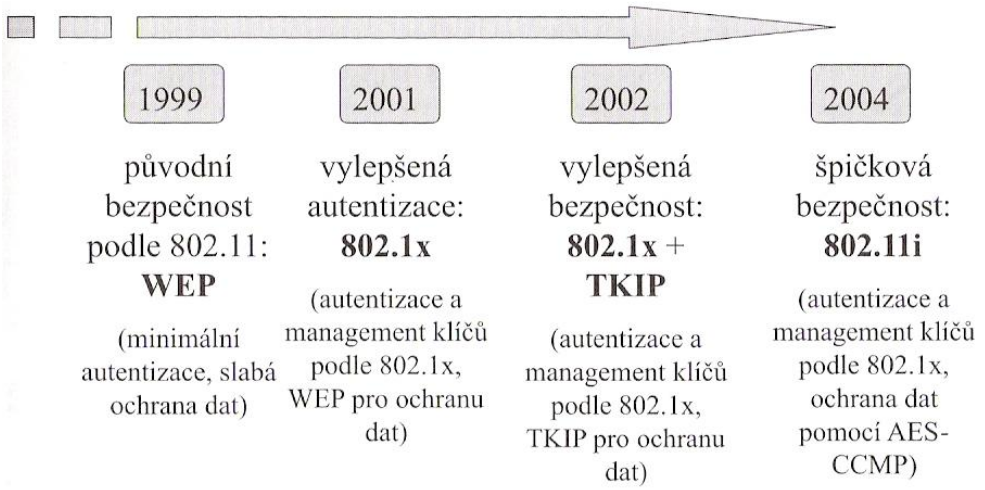
Bezpečností sítě se rozumí minimalizace zranitelných míst síťových prostředků. Ochranu v síti vyžadují:

- **Informace a data** (včetně dat spojených s bezpečnostními opatřeními, např. hesla).
- **Služby** přenosu a zpracování dat.
- **Zařízení**
- **Uživatelé**

Ohrožení komunikačního systému zahrnuje zničení, poškození, modifikaci, ukradení či ztrátu informací, případně zdrojů, odhalení soukromé informace, nebo přerušení služeb. K ohrožení může docházet neúmyslně nebo úmyslně („útoky“), zvenčí i zevnitř [2].

Bezdrátové sítě, Wi-Fi, nemají žádnou implicitně zabudovanou bezpečnost (implicitní je otevřený přístup k přístupovému bodu sítě), ale nabízejí zabezpečení jako nedílnou volitelnou možnost. Přesto mnohé firemní WLAN stále pracují zcela nezabezpečené, jak ukazují výsledky aktivit jako *warwalking, wardrivinng* nebo vizuálně dokreslené *warchalking* [2].

Od začátku implementace WLAN se pracuje na jejich lepším zabezpečení a v dnešní době jsou již k dispozici mechanismy, které dokáží zabezpečit WLAN i pro použití v nejpřísnějších podmínkách (např. vládní instituce). Vývoj řešení bezpečnosti WLAN je naznačen na obrázku (Obr. 8.).



Obr. 8. Vývoj podpory zabezpečení WLAN [2]

Bezpečnostní prvky v normě 802.11a/b/g se zaměřují pouze na autentizaci, šifrování a integritu dat. Autorizace není součástí specifikace a musí se provádět externími mechanismy (např. mechanismem pro řízení přístupu 802.1x) [2].

2.1 SSID

Přístupový bod vysílá implicitně identifikátor SSID (Service Set Identifier) každých několik sekund v takzvaném majákovém rámci (beacon frame). Takto může oprávněný uživatel snadno najít správnou síť, ale zároveň se do ní dostane i neoprávněný hacker. Právě díky této funkci dokáže většina softwarových detekčních nástrojů najít bezdrátovou síť bez předchozí znalosti SSID [9].

Hodnotu parametru SSID v síti je třeba považovat za první úroveň zabezpečení. Ve své základní, tovární, podobě nemusí SSID poskytovat žádnou ochranu proti neoprávněnému přístupu k síti, pokud jej ale změníme na hůře uhodnutelný text, nedostanou se vetřelci do sítě tak snadno, avšak za předpokladu, že je veřejné vysílání SSID vypnuto.

Tab. 2. Výchozí hodnoty SSID u některých výrobců

Výrobce	Výchozí hodnota SSID
3Com	101,comcomcom
Addtron	WLAN
Cisco	Tsunami, WaveLAN Network
Compaq	Compaq
Dlink	WLAN
Intel	101, 195, xlan, intel
Linksys	Linksys, wireless
Lucent/Cabletron	RoamAbout
NetGear	Wireless
SMC	WLAN
Symbol	101
Teletronics	any
Zcomax	any, mello, Test
Zyxel	Wireless
Ostatní	Wireless

Podrobný seznam SSID od všech výrobců, a dokonce i výchozí logovací jména a hesla k dalším síťovým zařízením, jsou dostupné na internetu. [9]

Vedle SSID se používá také ESSID (Extend Service Set Identification), který slouží jako jedna ze základních technik pro řízení přístupu klientů do WLAN. ESSID je hodnota naprogramovaná do AP pro identifikaci sítě (subnet), v níž se AP nachází. ESSID se nevysílá, takže přidružení do WLAN je povoleno pouze autorizovaným stanicím, které hodnotu identifikátoru znají. Síť používající ESSID se oprávněně označuje jako síť uzavřená [2].

2.2 Filtrování MAC adres

Metoda filtrování fyzických adres MAC představuje další možnost zabezpečení bezdrátových sítí. Adresa MAC síťové karty je 12ciferné hexadecimální číslo, které je jedinečné mezi všemi síťovými kartami na světě. Protože svoji adresu MAC má i každá bezdrátová karta sítě Ethernet, můžeme v přístupovém bodu snadno omezit povolení přístupu jen pro jistou množinu oprávněných zařízení a kohokoli cizího tak snadno vykázat ze sítě.

Filtrování adres MAC není ale bohužel úplně bezpečné, a plně se na ně spoléhat by bylo hrubou chybou [9].

Problém je totiž v tom, že řada bezdrátových karet mívá ovladač, který uživateli umožňuje MAC adresu změnit. Existují i jiné nástroje, které umožňují měnit MAC adresu. Protože se zdrojová a cílová adresa posílají nešifrovaně (a to i v případě použití WEP), může útočník jednoduše odposlechnout hodnoty povolených MAC adres a pak svou bezdrátovou kartu nastavit tak, aby používala takovouto platnou adresu. Když se karta tváří jako karta s povolenou MAC adresou, bude AP přesvědčeno, že jde o legitimní provoz. [1]

Kromě rizika falšování MAC adres se ve větších sítích stává neudržitelná administrace seznamu autorizovaných adres. Udržovat evidenci MAC adres všech karet, které ve vaší společnosti pořizujete nebo vyřazujete, a udržovat tento seznam aktualizovaný na všech AP, to je příliš mnoho práce v jakémkoli prostředí [1].

2.3 WEP

WEP není a ani neměl být žádným bezpečnostním algoritmem. Jeho úlohou nebyla ochrana dat ani před skriptovými amatéry, ani před inteligentnějšími útočníky, kteří se v síti zajímají o důvěrné údaje. Protokol WEP není konstruován k nějak zvlášť silnému zabezpečení, ale pouze zajišťuje, abychom si přechodem z pevné sítě „do vzduchu“ nesnížili bezpečnost dat (proto se také většinou vykládá jako Wired Equivalent Privaci, tedy „míra soukromí, ekvivalentní s pevnou sítí“). Problém je, že mnozí lidé vidí v jeho zkratce písmeno „E“ jako „Encryption“, šifrování. Úkolem WEP je vyřešit slabší zabezpečení bezdrátového přenosu oproti klasické pevné síti, to znamená, že *s protokolem WEP jsou data stejně bezpečná, jako na pevné, ale nešifrované síti typu Ethernet* [9].

2.3.1 Princip činnosti WEP

WEP funguje na symetrickém principu, kdy se pro šifrování a dešifrování používá stejný algoritmus i totožný statický klíč. Nejčastější (a nejslabší) 40-bitový klíč pro ověření totožnosti (autentizaci) je stejný pro všechny uživatele dané sítě (sdílený klíč) a klienti jej využívají spolu se svou adresou MAC pro autentizaci vůči přístupovému bodu.

Šifrování přenášených dat se provádí 64-bitovým klíčem, který je složen z uživatelského klíče a dynamicky se měnícího vektoru IV (Initialization Vector). WEP používá šifrovací algoritmus RC4.

2.3.2 Autentizace

Autentizace se provádí buď **otevřeně** (open system), nebo na základě **sdíleného klíče** (shared key).

- **Otevřená autentizace** není založena na žádném prověřování identifikačních údajů klienta. Ten pouze pošle svoji identifikaci přístupovému bodu a na základě tohoto požadavku jej přístupový bod přidruží. V rámci otevřené autentizace se může jakýkoli klient přidružit k přístupovému bodu.
- **Autentizace sdíleným klíčem** používá 40bitový uživatelský klíč, který je statický a stejný pro všechny uživatele dané sítě. Ve skutečnosti se ověřuje totožnost síťové karty, nikoli uživatele, což je jedna z hlavních slabin autentizace v rámci WEP.

Autentizace se provádí pouze jednostranně, nikoli vzájemně. Klienti nemají možnost žádat přístupový bod, aby se autentizoval.

Zvolený režim autentizace nemá přímou souvislost s šifrováním dat [2].

2.3.3 Šifrování

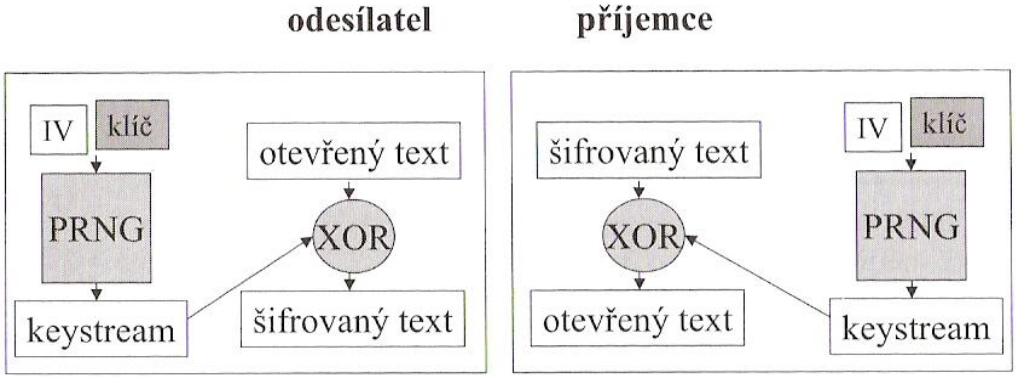
Informace o tom, že se používá šifrování WEP, je naznačená v záhlaví MAC rámce, nastavením bitu *Protecte Frame* v poli řízení rámce. Šifrování přenášených dat mezi klientem a přístupovým bodem se provádí 64bitovým nebo 128bitovým klíčem, který je složen z uživatelského (tajného) klíče v délce 40 respektive 104 bitů a dynamicky se měnícího inicializačního vektoru IV (*Initialization Vector*), vždy v délce 24 bitů. IV generuje vysílací strana, použije jej pro vytvoření šifry a současně jej pošle v otevřené formě jako součást záhlaví každého paketu. Příjemce použije IV přijatého rámce pro spojení se sdíleným WEP klíčem a provede dešifrování přijatých dat [2].

2.3.4 Šifra RC4

WEP používá RC4, symetrickou proudovou šifru vyvinutou v roce 1987 Ronaldem Rivestem (*Ron's Code No.4*). RC4 byla ve své době (konec 90. let) zvolena pro zabezpečení WLAN kvůli jednoduchosti implementace přímo do hardwaru síťového adaptéru, která má jen zanedbatelný dopad na výkonnost zařízení u většiny adaptérů. Proudová šifra umožňuje z klíče pevné délky vytvořit šifrovací proud (*cipher stream*) tak, aby bylo možné otevřený text libovolné délky převést do stejně dlouhého šifrovaného textu

(každému bitu textu odpovídá jeden bit šifry). RC4 dovoluje klíč o délce do 256 bitů, 802.11 pro WEP zvolilo délku 40 bitů.

RC4 pracuje jako generátor pseudonáhodných čísel (*PRNG, PseudoRandom Number Generator*), jehož základem je jedinečná kombinace tajného klíče a IV (Obr. 9.). Tajný klíč zůstává stejný, mění se periodicky jen IV. Výsledná pseudonáhodná posloupnost nul a jedniček se pro zašifrování spojí s otevřeným textem (daty) prostřednictvím logické funkce XOR. Dešifrování probíhá opět prostřednictvím funkce XOR použité na šifrovaný tok a zašifrovaný text. Funkce XOR totiž umožňuje opětovným použitím na výsledek získat původní hodnotu (RC4(X) XOR X XOR Y = RC4(Y)), proto hovoříme o RC4 jako o symetrické šifře. Jak uvidíme dále, právě tato vlastnost činí RC4, a tedy celý WEP, velice náchylným na útoky, a to i při částečné znalosti obsahu paketu ze strany útočníka.



Obr. 9. Šifrování RC4 [2]

2.4 IEEE 802.1X a EAP

O 802.1x se mnohdy hovoří různě: jako o bezpečnostní normě, protokolu, nebo dokonce autentizační metodě. Může se proto zdát, že 802.1X je samospasitelné řešení bezpečnosti (nejen v bezdrátových sítích). Skutečnost je poněkud méně optimistická, ale v každém případě je tato norma – novější než normy pro WLAN – při správné implementaci schopna přispět k lepšímu zabezpečení WLAN. Je třeba předeslat, že 802.1X nenahrazuje WEP, ale pracuje jako jeho nadstavba, a to pouze pro řízení přístupu.

IEEE 802.1X (Port Based Network Access Kontrol, 2001) je obecný bezpečnostní rámec pro LAN, zahrnující autentizaci uživatelů, integritu zpráv (šifrování) a distribuci klíčů. Autentizace se v případě WLAN realizuje na úrovní logických portů přístupového bodu (každá bezdrátová stanice komunikuje s jedním logickým portem AP na základě přidružení

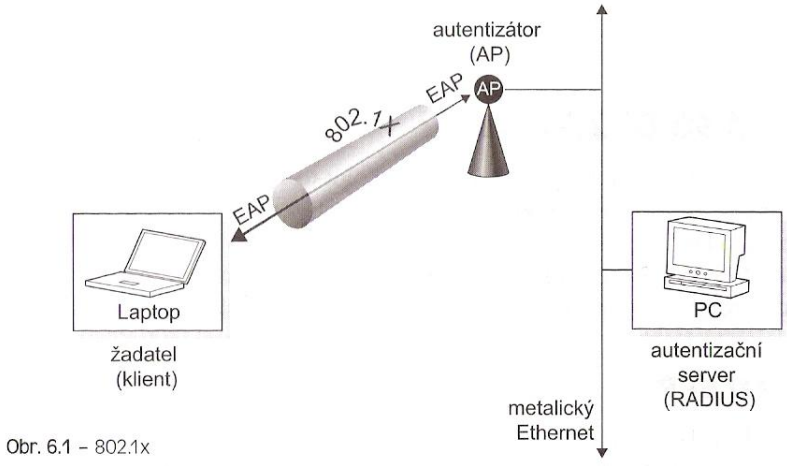
se k WLAN). Protokol 802.1X má za cíl blokovat přístup k segmentu lokální sítě pro neoprávněné uživatele. 802.1X slouží jako transport na spojové vrstvě pro zprávy autentizačního protokolu vyšší vrstvy (EAP) [2].

Protokol EAP (*Extensible Authentication Protocol*) byl původně vytvořen jako rozšíření protokolu PPP (Point-to-Pint Protocol, používaný u vytáčených připojení a některých DSL (Digital Subscribe Line) modemů, autentizuje pouze na základě jména a hesla). Základním cílem bylo vytvořit obecnou platformu pro různé autentizační metody. Jinak řečeno, jde o PPP se „zásuvnými" autentizačními moduly. Díky tomu můžete uživatele autentizovat tak, jak se vám zlíbí. Můžete používat hesla, certifikáty, tokeny, PKI (Publik Key Infrastructure), čipové karty, Kerberos (autentizační protokol), biometriky, (cokoliv jiného na co si vzpomenete), a tak dále. Otevřený standard zajišťuje, že kdykoliv v budoucnu budete moci metody zabezpečení zlepšit, protože jako nový typ EAP bude možno použít mechanismy, které dnes ještě ani neznáme [1].

802.1x má 3 základní komponenty :

- **Žadatel** : Uživatel nebo klient, požadující přístup k síti.
- **Autentizátor** : „Muž uprostřed", přepínač nebo AP, povolující nebo blokující provoz.
- **Autentizační server** : Systém udržující autentizační informace, typicky server RADIUS.

[1]



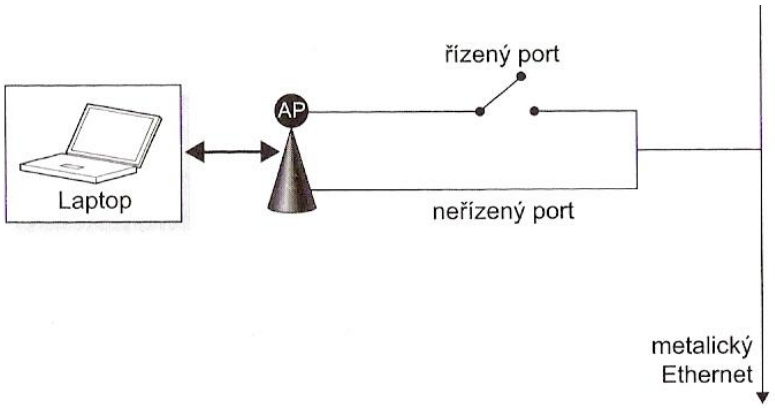
Obr. 10. Komponenty 802.1X [1]

Princip řízení přístupu je jednoduchý: jakmile chce klient získat přístup k LAN, autentizátor zablokuje veškeré síťové prostředky a služby pro klienta vyjma autentizačního serveru. Tak se klient musí nejprve autentizovat, než získá přístup do sítě.

Přístupové body tedy musí umožnit komunikaci po EAP pro klienta ještě před vlastní autentizaci. Proto se používá model tzv. duálního portu (Obr. 11.), kdy autentizátor podporuje dva porty:

- **Neřízený** (uncontrolled) – slouží pouze ke komunikaci autentizátora s autentizačním serverem.
- **Řízený** (controlled) – pro veškerý provoz autentizovaného/autorizovaného klienta.

[2]



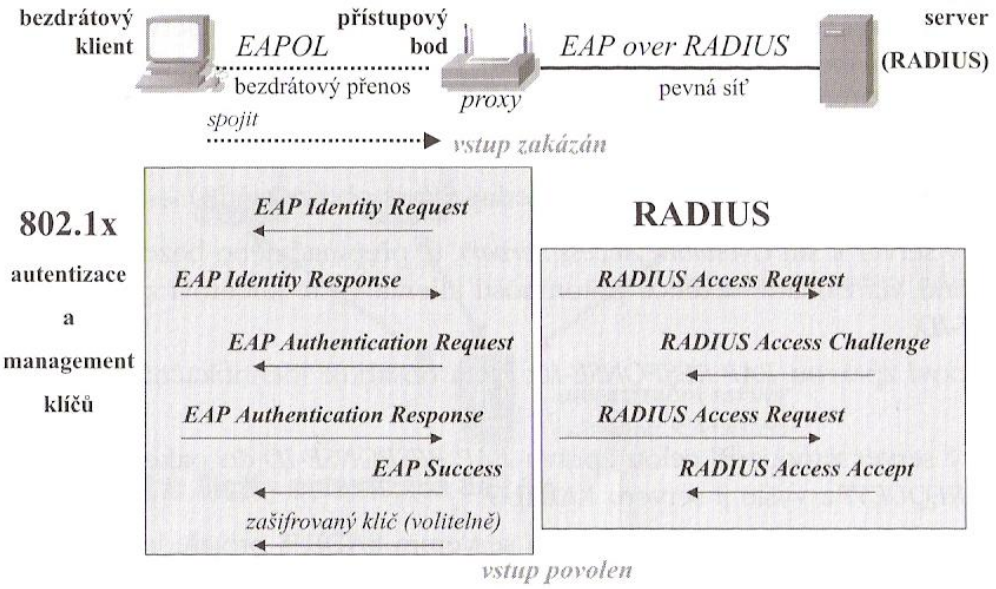
Obr. 11. Řízený a neřízený port [1]

2.4.1 Autentizace 802.1X

Autentizaci ve WLAN zprostředkovává přístupový bod pro klienty na základě jejich výzvy pomocí lokálního přístupového seznamu. Pouze ověřený uživatel má možnost přístupu k bezdrátové síti. Komunikace za účelem autentizace se ve skutečnosti skládá ze dvou částí: mezi klientem a přístupovým serverem a mezi přístupovým serverem a autentizačním serverem. Přístupový server je pouhým prostředníkem, který předává příslušné zprávy mezi klientem a autentizačním serverem a zpět.

Postup při autentizaci 802.1X je následující (Obr. 12.) :

- přístupový server k síti (Network Access Server), tj. přepínač nebo bezdrátový přístupový bod, na základě detekce přítomnosti klienta vyšle klientovi zprávu EAP REQUEST-ID.
- Klient odpoví zprávou EAP RESPONSE-ID, která obsahuje identifikační údaje uživatele.
- přístupový server zapouzdří celou zprávu EAP RESPONSE-ID do paketu RADIUS ACCESS_REQUEST a vyšle ji serveru RADIUS.
- zprávy EAP jsou posílány mezi klientem a serverem RADIUS prostřednictvím přístupového serveru: mezi klientem a AP jsou zapouzdřeny jako EAPOL a mezi AP a autentizačním serverem jako pakety RADIUS.
- server RADIUS odpoví zprávou obsahující povolení/zákaz přístupu pro daného klienta do sítě : RADIUS ACCESS_ACCEPT/DENY, která v sobě obsahuje informaci EAP SUCCESS/FAILURE, kterou přístupový server přepošle klientovi.
- v případě povolení přístupu (SUCCESS) je příslušný (logický) port přístupu do sítě (přes který autentizace probíhala) otevřen pro data daného uživatele, která je na základě úspěšného výše popsaného procesu považován za autentizovaného.



Obr. 12. Autentizace podle 802.1X [2]

Po úspěšné autentizaci následuje fáze správy klíčů, kdy přístupový bod distribuuje šifrovací klíče autentizovaným stanicím, a to prostřednictvím zprávy EAPOL-Key. Tato zpráva se může použít pro distribuci obou typů klíče. Zpráva se nepotvrzuje, takže při její ztrátě nebude mít žadatel a autentizátor stejné klíče a následná komunikace neproběhne v pořádku. Pak se musí provést autentizace celá znovu.

V rámci procesu autentizace se generují dvě sady klíčů (128 bitových) :

- **párové klíče** (*pairwise*) jedinečné pro spojení mezi přístupovým bodem a klientem – zajištění spoje a překonání stejného klíče pro všechny u WPA, **PMK** (*Pairwise Master Key*) je jedinečný pro relaci mezi žadatelem a autentizačním serverem.
- **skupinové klíče** (*groupwise*) sdílené všemi stanicemi v jedné buňce 802.11 – používané pro šifrování skupinové komunikace (*multicast*).

[2]

2.4.2 Autentizační metody protokolu EAP

V současné době protokol EAP podporuje desítky metod autentizace. Následujících pět patří mezi ty nejrozšířenější. Od zvolené metody se odvíjí jak náročnost její implementace, tak i bezpečnost celého řešení. Některé metody se instalují snáze, jiné jsou zase mnohem bezpečnější. Zvolenou metodu autentizace EAP musí podporovat všechny tři komponenty systému – žadatelé, autentizátoři i autetizační server [1].

- **EAP-MD5 –** Metoda EAP-MD5 (Message Digest) se při odesílání autentizačních informací na server RADIUS opírá o haš (otisk) MD5, vytvořený z uživatelského jména a hesla. Tato metoda nezajišťuje žádnou správu klíčů ani nenabízí dynamické generování klíčů WEP, a proto vyžaduje statické klíče WEP. Díky tomu se EAP-MD5 považuje za nejméně bezpečnou metodu EAP.
- **LEAP** (Lightweight Extensible Authentication Protocol) **-** Metodu EAP-Cisco Wireless, označovavá častěji jako LEAP, vyvinula na základě normy 802.1x firma Cisco a je základem velké části oficiálně schválené verze EAP. Podobně jako EAP-MD5 i metoda LEAP od klientského bezdrátového zařízení přebírá uživatelské jméno a heslo, a předává je k autentizaci na server RADIUS. Firma Cisco doplnila kromě požadavků samotné normy i další podporu

a přinesla tak do metody vyšší bezpečnost. U autentizační metody LEAP je v současné době známo jediné omezení; pro autentizaci klientů i přístupového bodu se používá protokol MS-CHAPv1 (Microsoft Challenge-handshake authentication protoco version 1), který obsahuje známá zranitelná místa.

- **EAP-TLS** (Transport Layer Security) – Metodu EAP-TLS vyvinula firma Microsoft a její popis je uveden v dokumentu RFC 2176. Namísto kombinace uživatelského jména a hesla provádí tato metoda autentizaci pomocí certifikátů X.509; informace veřejného klíče v PKI se zde do EAP přenášejí pomocí zabezpečení transportní vrstvy. Tuto metodu má smysl uvádět do provozu jen v případě, že se při její implementaci budeme přesně držet doporučení firmy Microsoft.
- **EAP-TTLS** (Tuneled Transport Layer Security) – Autentizační metodu EAP-TTLS zavedla firma Funk Software, a to jako alternativu k výše popsané EAP-TLS. Bezdrátový přístupový bod se i zde musí autentizovat vůči klientu pomocí serverového certifikátu, ale uživatelé odesílají pro přihlášení jen uživatelské jméno a heslo. Tyto přihlašovací údaje pak EAP-TTLS předává k ověření pomocí libovolného mechanismu výzvy a odpovědi, určeného administrátorem (PAP, CHAP, MS-CHAPv1, MS-CHAPv2, PAP/totenová karta, nebo EAP)

[9]

- **PEAP** (Protected EAP) - Protokol PEAP používá protokol TLS k vytvoření zašifrovaného kanálu mezi ověřovaným klientem protokolu PEAP, například počítačem v bezdrátové síti, a ověřovatelem protokolu PEAP, například server RADIUS. Protokol PEAP neurčuje metodu ověřování, ale poskytuje další zabezpečení ostatních protokolů ověřování EAP, například protokolu EAP MSCHAPv2, který může pracovat prostřednictvím zašifrovaného kanálu protokolu TLS poskytnutého protokolem PEAP. Proces ověřování pomocí protokolu PEAP mezi klientem a ověřovatelem tohoto protokolu se skládá ze dvou fází. Během první fáze je vytvořen zabezpečený kanál mezi klientem a ověřujícím serverem protokolu PEAP. V druhé fázi dojde mezi klientem a ověřovatelem protokolu EAP k ověřování pomocí protokolu EAP [21].

2.5 WPA

31. října 2002 ohlásila Wi-Fi aliance protokol WPA (Wi-Fi Protected Access), což je v zásadě kompromisní řešení, protože některé části specifikace 802.11i už byly hotovy (například 802.11y a TKIP, tedy Temporary Key Integrity Protocol), zatímco jiné ještě ne (například AES, Advanced Encryption Standard a zabezpečená deautentizace a disasociace).

Logika, kterou se Wi-Fi asociace řídila, byla prostá: Nemůžeme čekat do doby, než dojde k ratifikaci 802.11i, což se stane přinejlepším za rok nebo dva[1], takže vezmeme to, co už je hotovo a vydáme to hned. WPA je tak podmnožinou 802.11i, kterou lze implementovat prostřednictvím aktualizace softwaru a firmwaru. Řeší jak šifrování (TKIP), tak řízení přístupu (802.1x). Z bezpečnostního pohledu mají tyto technologie značný význam, protože řeší řadu slabin a bezpečnostních děr protokolů WEP a 802.11 [1].

Pro WPA je potřeba :

- Přístupový bod s podporou pro WPA.
- Bezdrátová karta s ovladači pro WPA.
- Klient s podporou WPA v operačním systému.

WPA tvoří následující 3 složky:

- **Temporary Key Integrity Protocol** (TKIP): používá 40bitový klíč jako WEP (s RC4), ale mění jej pro každý paket a brání se tak proti útoku hrubou silou, navíc se zdvojnásobila délka IV na 48 bitů.
- **Message Integrity Check** (MIC): přenos je chráněn proti narušení, integrita dat zajištěna (ochrana proti falešným přístupovým bodům).
- **Extensible Authentication Protocol** (EAP): vzájemná autentizace uživatele i sítě (ochrana proti falešným přístupovým bodům) a distribuce klíčů.

[2]

[1] Ke schválení došlo v roce 2004

2.5.1 TKIP

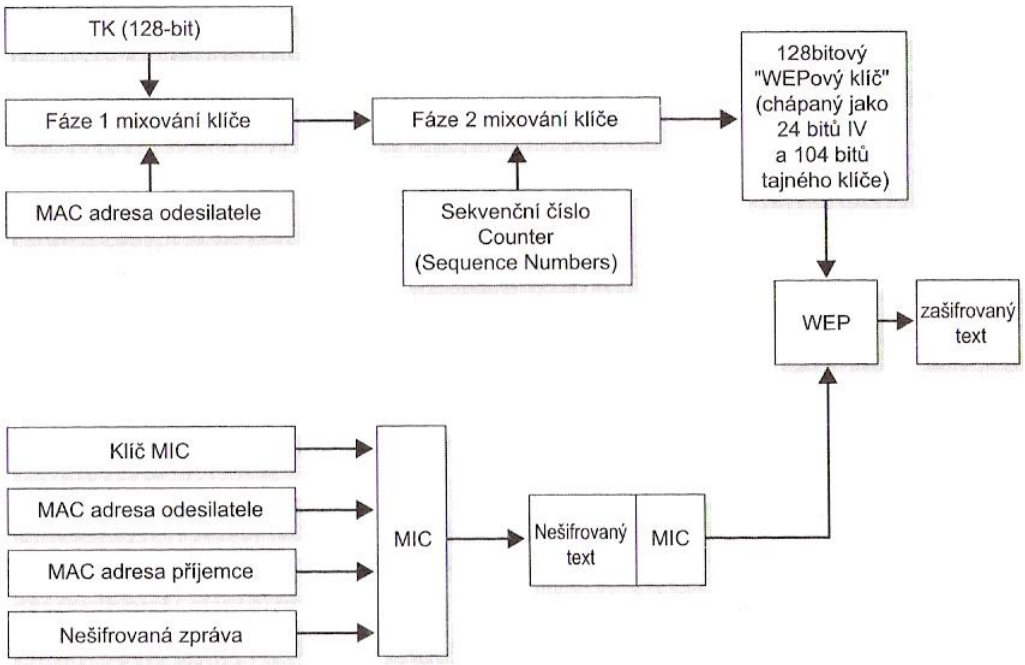
Mechanismus TKIP zlepšuje šifrování prostřednictvím tří hlavních prvků:

- Funkce mixování klíče pro každý paket.
- Vylepšená funkce kontroly integrity (MIC, Message Integrity Code), pojmenovaná Michael.
- Vylepšená pravidla generování IV včetně sekvenčních pravidel.

V zásadě představuje TKIP pouze dočasnou opravu protokolu WEP. Kvůli zachování zpětné kompatibility s velkým počtem stávajících instalovaných hardwarových zařízení byly při jeho návrhu učiněny různé kompromisy. Představuje však řešení všech známých problémů protokolu WEP.

U TKIP klient začíná s dvěma klíči – 128bitovým šifrovacím klíčem a 64bitovým klíčem pro zajištění integrity, které získá bezpečnými mechanismy v průběhu iniciální komunikace protokolem 802.1x. Šifrovací klíč se označuje jako TK, Temporary Key. Klíč pro zajištění integrity se označuje jako klíč MIC, Message Integrity Code. V první fázi se provede XOR mezi MAC adresou odesilatele a hodnotou TK, čímž vzniká klíč označovaný jako Fáze 1 (někdy též „mezilehlý klíč“). Klíč Fáze 1 se mixuje se sekvenčním číslem a vzniká tak klíč Fáze 2, pro přenos jediného paketu. Výstup druhé fáze se předává mechanismu WEP jako standardní 128bitový WEPový klíč (ted IV + tajný klíč). Zbytek procesu už probíhá jako klasická transakce protokolem WEP.

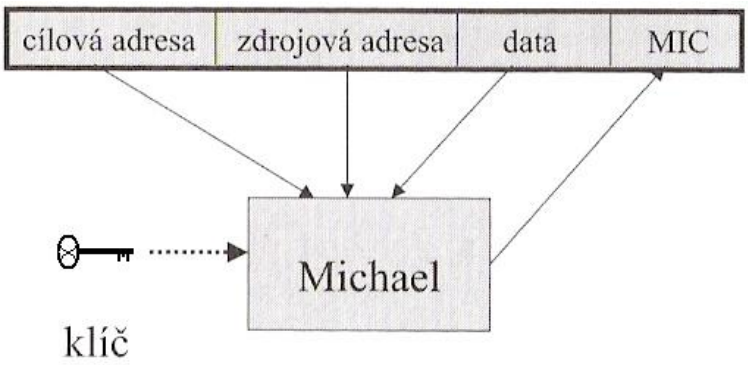
[1]



Obr. 13. Šifrování mechanismem TKIP [1]

2.5.2 MIC

Namísto jednoduché 32bitové hodnoty CRC (Cyclic Redundancy Check) se v TKIP ke kontrole integrity používá funkce Michael (MIC), jednocestná hashovaní funkce, navržená Neilsem Fergusonem. Nejde o lineární funkci a pro útočníka je tak velmi obtížné při přenosu paket modifikovat. Michael vyžaduje následující vstupy: klíč MIC, zdrojovou adresu, cílovou adresu a nešifrovaný text. Tím, že pracuje i se zdrojovou a cílovou adresou, je možné ověřit integritu MAC adres. Výstup algoritmu Michael je dlouhý 8 bajtů a připojuje se k přenášeným datům.



Obr. 14. Výpočet MIC [2]

2.6 802.11i (WPA2)

Jak ji bylo řečeno, WPA je dočasné opatření, které v polovině roku 2003 umožnilo v praxi nasadit část výsledků práce skupiny 802.11i. WPA je tedy podmnožinou standardu 802.11i. Primární komponenta protokolu 802.11i, která v té době ještě nebyla úplně hotova, byla šifra AES (Advanced Encryption Standard). Ve specifikaci 802:11i je AES povinné, zatímco TKIP pouze volitelné [1].

2.6.1 Šifra AES

AES je šifra odpovídající americkému federálnímu standardu FIPS (Federal Information Processing Standards), která byla navržena jako náhrada za šifru RC4. Samotnému přijetí šifry AES americkou vládou předcházel rozsáhlý průzkum a revize šifry.

AES nabízí různé režimy činnosti, ve specifikaci 802.11i se používá čítačový režim s protokolem CBC-MAC (CCM), obvykle označovaný jako AES-CCMP. Čítačový režim zajišťuje šifrování, CBC-MAC pak zajišťuje autentizaci a integritu dat.

Stejně jako RC4 je i AES šifra se symetrickým klíčem, což znamená, že se text šifruje i dešifruje stejným sdíleným tajným klíčem. Na rozdíl od šifry RC4, která šifruje lineárně každý bajt XORováním s náhodnou sekvencí, AES pracuje s vloky o velikosti 128 bitů a proto se označuje jako bloková šifra.

CCMP i TKIP mají řadu společných vlastností. Oba používají 128bitový dočasný klíč, odvozený od „master“ klíče, který se získává v průběhu negociace protokolem 802.11x. V terminologii CCMP se 48bitová hodnota IV označuje jako „číslo paketu“.

[1]

2.6.2 Nový MIC

Stejně jako TKIP i CCMP obsahuje algoritmus MIC zajišťující, že nedošlo k modifikaci přenášených dat. Nicméně mechanismus MIC v CCMP funguje jinak, než algoritmus Michael v TKIP. Výpočet MIC je založen na inicializačních hodnotách vycházejících z IV a z dalších hlavičkových informací. Pracuje ve 128bitových blocích a počítá se přes jednotlivé bloky až na konec originální zprávy, kdy se vypočte konečná hodnota [1].

2.6.3 Nový šifrovací mechanizmus

Čítačový režim šifrování šifrou AES se výrazně liší od WEP/TKIP a RC4. Výstupem šifry AES je po inicializaci (založené na IV a dalších hlavičkových informacích) jen 128birový blok. Celý vstupní text se rozdělí na 128bitové bloky a ty se postupně XORují se 128 bitovým pokaždé nově generovaným výstupem AES tak dlouho, dokud nedojde k zašifrování celé původní zprávy. Nakonec se čítač vynuluje, XORuje se hodnota MIC, která se přidává na konec rámce.

Výsledkem je mnohem silnější šifra. Zvýšené šifrovací nároky by ovšem přetížily procesory stávajících zařízení založených na WEP/RC4. Z toho důvodu vyžaduje AES nový hardware, a je tedy nekompatibilní s první generací bezdrátových zařízení.

[1]

3 HARDWAROVÉ PRVKY BEZDRÁTOVÝCH SÍTÍ

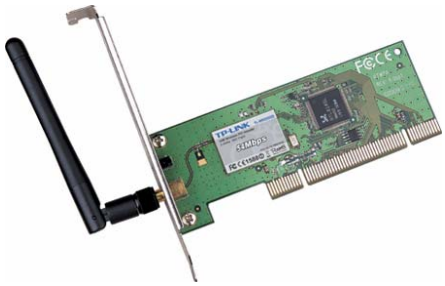
V dnešní době už existuje nespočet výrobců hardwaru, kteří ve svém sortimentu nabízí prvky umožňující jak vytvoření nebo připojení se k bezdrátové Wi-Fi síti, tak i zařízení používající bezdrátovou Wi-Fi síť ke komunikaci. Následující kapitola obsahuje stručný přehled zařízení, které slouží k vytvoření a připojení se k bezdrátové Wi-Fi síti.

3.1 Integrované bezdrátové síťové karty

Nejčastěji se s nimi setkáte v mobilních zařízeních, jako jsou notebooky, PDA ale také tzv. „chytré“ mobilní telefony. Tyto zařízení mívají chip karty implementován přímo na základní desce a anténu zabudovanou v konstrukci, což v případě přenosných počítačů představuje kvalitní zisk signálu i na větší vzdálenost od vysílače. U menších zařízení, jako jsou právě PDA nebo mobilní telefony je však třeba být ve větší blízkosti zdroje signálu.

3.2 Interní bezdrátové síťové karty

Těmito síťovými kartami lze rozšířit komunikační rozhraní u zařízení, které nejsou z výroby vybaveny bezdrátovou Wi-Fi technologií, ale umožňují připojení karet přes některou z dnes běžně používaných komunikačních sběrnic pro připojení interních rozšiřujících karet jako jsou sběrnice miniPCI, PCI a PCI-Express. Tyto karty bývají vybaveny konektorem pro připojení externí antény. Levnější modely mívají anténu připojenou napevno bez možnosti její demontáže.



Obr. 15. Bezdrátová karta do sběrnice PCI

Obr. 16. Bezdrátová karta do sběrnice miniPCI

3.3 Externí bezdrátové síťové karty

Externí bezdrátové síťové karty plní stejnou funkci jako karty interní, které byli popsány v předešlé kapitole. Zásadně se však liší svou konstrukcí a rozhranními, které používají ke komunikaci se zařízením, ke kterému jsou připojeny.

Tyto karty bývají ukryty v pevné konstrukci a ke komunikaci využívají rozhranní typu USB nebo sběrnici PCMCI. Nejčastěji se používají ve spojení s přenosnými počítači. Většinou mívají integrovanou anténu pro příjem signálu, která však nijak neoslní svou ziskovostí a je třeba být v dosahu kvalitního signálu. Dražší provedení již bývají vybaveny například vysouvací anténou nebo konektorem pro připojení antény externí.

Obr. 17. Bezdrátová karta do USB a PCMCI

3.4 Bezdrátové accesspointy

Bezdrátový Access Point (AP) již byl krátce zmíněn v kapitole 1.3.2 jako jeden z prvků bezdrátové sítě, který obstarává přechod mezi metalickou a bezdrátovou částí sítě. Tento popis podstatě vystihuje jeho základní funkci. AP však může obstarávat i řadu dalších funkcí. Tyto zařízení budou popsána v další kapitole.

Pokud se však jedná pouze o bezdrátový AP, jde o zařízení vybavené zpravidla jedním konektorem RJ-45, konektorem pro připojení externí antény, konektorem pro připojení napájecího adaptéru, tlačítkem „reset“ , které uvede zařízení do továrního nastavení a několika signalizačními diodami. Tato zařízení se spravují převážně přes webové rozhraní a lze je nastavit do módů Access point, Klient a Bridge.

Počet klientských stanic, které lze připojit k jednomu AP je teoreticky omezen pouze rozsahem provozované sítě. U některých výrobců bývá optimální počet stanic uveden v popisu zařízení, obecně však lze říct že je to max. do 10 stanic u levnějších zařízení a až 254 u těch nejdražších. Dále je třeba vzít v potaz skutečnost, že všechny připojené stanice se dělí o jednu šířku pásma, tudíž se vzrůstajícím počtem aktivních připojených klientů klesá rychlost připojení. Dále pak může docházet k výpadkům AP či jeho samovolným restartům.

Obr. 18. Bezdrátový AccessPoint

3.5 Multifunkční bezdrátová zařízení

Tyto zařízení poskytují svým uživatelům oproti klasickým Access pointům mnoho dalších funkcí, jako router, DHCP server, ftp server, print server, firewall. K další výbavě těchto

zařízení patří switch, většinou se 4 porty a také jeden port pro připojení WAN sítě. Některá tyto zařízení mohou mít integrován DSL modem nebo modem pro GPRS/EDGE sítě.

Dražší modely těchto zařízení mohou být vybaveny i USB porty, což z nich činí velice zajímavá zařízení. Lze k ním například připojit tiskárnu, externí HDD nebo web-kameru přímo přes rozhranní USB. Odpadá tak nutnost pořizování dražších modelů se síťovým rozhranním.

Obr. 19. Multifunkční bezdrátové zařízeni ASUS

3.6 Antény

Anténa obecně je zařízení, které dokáže energii, která je k ní přivedena, vyzářit do prostoru kolem sebe a vytvořit tak elektromagnetické pole o určité frekvenci - vysílač. Dále pak, pokud jsou umístěny do prostředí elektromagnetického pole, jsou schopny přijímat signál z tohoto pole – přijímač.

Antény dodávané s jednotlivými Wi-Fi prvky postačují pro použití uvnitř budov, ale na větší dosah vhodné nejsou. Lze sice namítnout, že Wi-Fi je primárně určeno pro výstavbu sítí uvnitř budov, ale lze je též výhodně použít i k propojování budov. V poslední době, a zejména kvůli situaci na českém telekomunikačním trhu, se Wi-Fi uplatňuje rovněž jako řešení problému „poslední míle“, tedy jako distribuce internetového připojení. A s rozmachem komunitních sítí se také s oblibou používá pro propojování vzdálenějších bodů – výjimkou nejsou i pětikilometrové vzdálenosti, které se překlenují pomocí Wi-Fi a směrových antén [3].

Antény mají celou řadu vlastností, z nichž se odvíjejí jejich provozní a výkonnostní charakteristiky:

- **Frekvence:** Každá anténa je vhodná pro konkrétní frekvenci. Frekvence používané u Wi-Fi sítí je popsána v kapitole 1.2.
- **Výkon:** Antény počítají s určitým maximálním vyzařovaným výkonem (ve wattech).
- **Směrovost:** Každá anténa formuje vyzařované pole do určitého směru.
- **Polarizace:** Udává rovinu, ve které anténa vysílá signál.
- **Zisk:** Používá se ke změření množství signálu, který anténa vysílá nebo přijímá a je vyjádřena poměrovým systémem. Měří se v decibelech (dB).

[1]

3.6.1 Polarizace antén

Rovina polarizace udává směr, ve kterém bude daná anténa vyzařovat/přijímat signál. Tato vlastnost je dána výhradně vnitřním konstrukčním uspořádáním antény. U bezdrátových sítí se používají dva druhy polarizace, lineární a kruhová.

Lineární polarizaci můžeme dále rozlišit na lineárně horizontální (sinusoida signálu se pohybuje z leva doprava a zpět) a lineárně vertikální (sinusoida se pohybuje shora dolů a nazpět). Horizontální polarizace se zpravidla používá u všesměrových antén. U antén směrových lze polarizaci jednoduše změnit pootočením antény o 90°. Signál horizontálně polarizovaný a vertikálně polarizovaný se vzájemně téměř neruší.

U kruhové polarizace jde podstatě o spojení horizontální a vertikální polarizace. Sinusoida signálu se točí ve spirále. Podle směru otáčení rozlišujeme polarizaci levotočivou a pravotočivou. Tento druh polarizace je nejvíce odolný vůči rušení, avšak ruší spoje obou lineárních polarizací.

3.6.2 Směrovost antén

Každá anténa vysílá svůj signál do určitého směru a pokrývá tak svým signálem určitou oblast. Podle toho, do jakých směrů antény signál distribuují, dělíme je na isotropní, směrové, všesměrové a sektorové.

Isotropní antény jsou základním typem antén. Jejich konstrukce je pouze teoretická a slouží jako referenční rámec pro měření vlastností reálných antén. Hypotetická isotropní

anténa vyzařuje energii ve všech směrech stejně. Můžeme si ji představit jako bod v prostoru, který vyzařuje energii do všech směrů.. Isotropní anténa nemá žádné fyzické části (jako třeba vodiče), prostě jen distribuuje energii v úhlu 360° [1].

Směrové antény, jak již název napovídá, směrují vysílání/zisk, jedním směrem. Používají se jako klientské a nebo na bezdrátové spoje. Konstrukčně je lze rozdělit na YAGI antény a parabolické reflektory.

YAGI antény, přesným názvem Podélné anténní soustavy, jsou dlouhé tyče s několika sfázovanými půlvlnnými dipóly, které vzájemně rezonují a tím zesilují přijímaný či vysílaný signál. Tyto antény jsou kompaktnější avšak mývají horší fyzikální vlastnosti.

Parabolické reflektory jsou tvořený zářičem a parabolickým reflektorem. Samotné parabolické reflektory bývají konstruovány jako síto nebo plná parabola. Parabola soustředí signál vyzářený zářičem do úzkého paprsku. Tyto antény dosahují vysokého zisku, obzvláště pak ty z plnou parabolou, neboť vykazují minimální postraní a zadní vyzařování.

Obr. 20. Bezdrátové antény: YAGI, parabolický reflektor a síto

Všesměrové antény vyzařují v horizontálním úhlu 360°, vertikálním 10 – 20°. Z toho vyplývá, že prostor nad a pod anténou není pokryt signálem. Zisk těchto antén se pohybuje okolo 10 dB. Konstrukčně bývají tvořeny kovovým vodičem uvnitř plastového obalu u levnějších variant nebo soustavou sfázovaných zářičů u dražších variant. Tyto antény jsou nejběžněji používanými anténami dodávanými přímo výrobcem k jednotlivým zařízením.

Obr. 21. Všesměrová anténa

Sektorové antény vyzařují do určitého úhlu, například vykrývají úhel 180° nebo jen 60°. Používají se tam, kde je třeba vykrýt pouze specificky omezené oblasti a je třeba i vhodné zabránit pronikání signálu mimo požadovanou oblast. Například na zeď budovy je vhodné umístit anténu se směrovým vyzařováním 180° pro pokrytí místnosti a na vykrytí roku použijeme anténu s vyzařováním pouze 90° [3].

Tyto antény mají rovněž kompaktní rozměry – bývají silné jen několik centimetrů a lze je snadno montovat na zeď. Toto je důležité zejména u vnitřních instalací, kde hraje svoji roli i estetické hledisko [1].

3.6.3 Zisk

Zisk představuje „nejdůležitější“ parametr antény. Jednoduše řečeno, čím vyšší ziskovost, tím vzdálenější signál je anténa schopna zachytit. Technicky řečeno se jedná o poměr mezi intenzitou vyzařování v daném směru k intenzitě vyzařování, kterou bychom obdrželi, kdyby energie přijatá anténou byla vyzářena rovnoměrně do všech směrů, tedy takzvanou izotropní anténou nebo reálným půlvlnným dipólem.

Zisk antény se udává v dBi, tedy v decibelech na izotop nebo méně často v dBd, tedy v decibelech na dipól, podle toho, k jakému typu antény je měření vztahováno. Pro stejnou anténu je velikost zisku v dBi o 2,16 dB větší než údaj v dBd. Snad také proto většina výrobců uvádí velikost zisku svých antén v dBi.

[3]

II. PRAKTICKÁ ČÁST

4 ANALÝZA PRAKTICKÉ VÝUKY BEZDRÁTOVÝCH SÍTÍ NA FAI

Výuka sítí obecně probíhá v současné době na Univerzitě Tomáše Bati, Fakultě aplikované informatiky, ve dvou na sebe navazujících povinných předmětech, a to Počítačové sítě v 4. Semestru bakalářského studia a Provoz počítačových sítí v 5. Semestru navazujícího magisterského studia. Vedle těchto povinných předmětů mají studenti možnost zapsat se na nepovinně volitelné předměty CISCO 2-Směrovače a základy směrovačů v 5. semestru Bc. studia. Dále se chystá zavedení kurzů CISCO 3-Přepínání a pokročilé směrování v 6. semestru Bc. studia a CISCO 4-Technologie WAN v 7.semestru Ing studia.

V rámci předmětu, Počítačové sítě, se studenti seznamují s historií a dělením počítačových sítí, topologiemi, přístupovými metodami, modelem ISO/OSI, protokolem TCP/IP, modulacemi signálu, přenosovými médii, základy Ethernetu a bezdrátovými sítěmi. V rámci bezdrátových sítí se probírají jednotlivá frekvenční pásma, jak licenční tak bezlicenční, dále pak topologie, prvky bezdrátových sítí a metody zabezpečení. To vše však pouze teoreticky na přednáškách. V rámci cvičení studenti absolvují kurz CISCO CCNA Exploration - Network Fundamentals a v případě úspěšného absolvování závěrečného testu získají příslušný certifikát.

Cílem navazujícího předmětu Provoz Počítačových sítí je představit studentům počítačové sítě z pohledu správce sítě. Postupně je na přednáškách probírána problematika mobilních sítí GSM a UMTS, připojení jednotlivých PC a malých sítí do Internetu, DNS systému a konfigurace DNS serverů, firewalů, překladu adres, směrování v sítích. Na závěr jsou posluchači seznámení s problematikou záložních zdrojů. Teoretické znalosti jsou ověřovány v laboratořích na CAN Ethernet s programovým vybavením Linux a Microsoft Windows. Dále jsou teoretické znalosti ověřovány v Internetu a na směrovačích a přepínačích firmy Cisco.

V nepovinně volitelném předmětu CISCO 2-Směrovače a základy směrovačů studenti absolvují navazující kurz Cisco CCNA 2 – Směrovací protokoly a koncepty. V laboratořích si studenti prakticky vyzkouší konfiguraci a práci přímo se směrovači Cisco. Po absolvování všech dílčích testů a úspěšném zvládnutí testu závěrečného obdrží příslušný certifikát.

Chystaný předmět CISCO 3 posluchače seznámí s problematikou kurzu Cisco CCNA Exploration - LAN přepínání a bezdrátové technologie. Další chystaný předmět CISCO 4

pak bude navazovat a posluchači absolvují kurz Cisco CCNA Exploration - Připojení k síti WAN. V rámci laboratoří těchto dvou předmětů studenti absolvují praktická cvičení na směrovačích a přepínačích Cisco, jednotlivé dílčí testy a závěrečný test. Po úspěšném absolvování předmětu posluchači získají příslušný CISCO certifikát.

Pomineme-li tedy oba chystané nepovinně volitelné předměty, s bezdrátovými sítěmi se studenti seznamují již ve 4 semestru, ovšem pouze teoreticky. Ve cvičeních tohoto kurzu se totiž studenti již prakticky nezkoušejí znalosti získané z přednášek, ale absolvují kurz Cisco. Toto řešení dle mého názoru není nejšťastnější, neboť informace získané z kurzu a absolvování testů nenahradí praktické zkušenosti, které by mohly studenti získat, pokud by na cvičeních byla prakticky procvičována probíraná látka. Navíc, pokud student nepokračuje navazujícími Cisco kurzy, získaný certifikát pozbývá významu. Mnohem efektivnější by bylo i tento Cisco kurzy vyčlenit do nepovinně volitelného předmětu, jak je to v případě kurzu CISCO 2, 3 a 4. Otevřela by se tím možnost prakticky cvičit přímo problematiku, která je probírána na přednáškách a tedy i bezdrátové sítě.

Pokud tedy pominu ostatní probíranou látku a zaměřím se pouze na bezdrátové sítě, studenti mají po absolvování předmětu Počítačové sítě povědomí o bezdrátových sítích, zejména pak o sítí 802.11 a Wi-Fi. Ví, na jakých pracují frekvencích a dokážou se k již existující bezdrátové síti připojit. Ovšem to vše spíše díky tomu, že v poslední době se k nezabezpečené bezdrátové síti mohou připojit téměř všude. Pokud ovšem mají bezdrátovou síť navrhnout, sestavit a nakonfigurovat jednotlivá zařízení jako je Access point nebo Wi-Fi router a vytvořenou síť následně efektivně zabezpečit, tak jim praktické zkušenosti z výuky mohou znatelně chybět a z vlastní zkušenosti vím, že někteří studenti by si konfigurací Access pointu naprosto nevěděli rady.

Tato situace, dle mého názoru, není ideální, neboť bezdrátové sítě a zejména pak sítě 802.11 se pomalu stávají samozřejmostí, ať už jako možnost připojení se k internetu na veřejném místě, či jako poslední míle komerčního poskytovatele internetu a absolvent vysoké školy by měl zvládnout bezdrátovou síť nejen navrhnout ale také realizovat alespoň na úrovni malé domácí sítě nebo připojení sítě do internetu.

5 NÁVRH VYBAVENÍ LABORATOŘE

Jelikož mezi dnes nejrozšířenější bezdrátové sítě patří sítě 802.11b/g, bude laboratoř vybavena bezdrátovými prvky odpovídajícími tomuto standardu. Bylo uvažováno i zařazení prvků standardu 802.11a ale jejich technologie a administrace je podstatě shodná a liší se pouze vysílací frekvencí a vyšší pořizovací cenou.

Laboratoř bude obsahovat celkem 10 odborných pracovišť vybavených stolními počítači pro laboratorní výuku bezdrátových počítačových sítí. Všechna pracoviště budou propojena sítí Ethernet 100 Mbps do centrálního switche umístěného v laboratoři. Dále pak bude vybavena aktivními WiFi přístupovými body a WiFi routery rovněž připojenými do centrálního switche. Switch bude připojen k 3 portovému routeru Mikrotik, který bude zároveň zastávat funkci DHCP serveru, vysílat bezdrátovou síť „wifi_ucebna“ a také zprostředkovávat spojení s autentizačním RADIUS serverem. Router bude možné přes volný port RJ-45 volitelně připojit do školní sítě.

5.1 Návrh hard-warových prvků

5.1.1 PC BAREBONE 4500

- Foxcon G31MXP-K
- Intel Celeron P430 1,80GHz (512/800)
- DDR2 1024MB 800 MHz BAR TRANSCED
- Integrovaná Intel GMA 3100
- HDD SEAGATE BARRACUDA 160GB SATAII/300 8MB, 7200
- DVD RW Samsung Blafl S223B/BEBE 22xDrive
- Gigabit Lan, Realtek® RTL8111B/RTL8111D
- D-Link DWL-G520 AirPlus XtremeG 11/54/108Mb/s
- OS Win XP
- ACER 17“ LCD V173Bb 1280x1024,7000:1,250cd/m2,5ms
- Genius LuxeMate 300 USB/PS2
- Genius Net Scroll 200 Laser PS2 1600dpi

- Cena sestavy bez DPH: 9936,-
- Cena sestavy s DPH: 11823,-

5.1.2 OvisLink AirLive WL-5460

- Komunikační porty: 2x RJ-45 (10/100 Mbit/s)
- Konfigurace: Web management, SNMP
- Pracovní teplota [°C]: 0-60
- Rozměry [mm]: 135 x 100 x 26
- Hmotnost [g]: 180
- Podporované specifikace WLAN: IEEE 802.11b, IEEE 802.11g
- Anténa: 2 dBi odpojitelná dipólová
- Přenosové rychlosti: 1/2/5.5/11 Mbit/s, 18 Mbit/s, 24 Mbit/s, 36 Mbit/s, 48 Mbit/s, 54 Mbit/s
- Šifrování: WEP 64/128-bit, WPA, WPA 2
- Funkce access poitu: Bridge, Client, Repeater
- Výstupní výkon [dBm]: 18
- Cena bez DPH: 776,-
- Cena s DPH: 924,-

5.1.3 D-Link DI-524 AirPlusG

- 11/54Mbps Wireless LAN Access Point
- Compatible with IEEE 802.11b/802.11g (DSSS) 2.4GHz Standard
- 64-/128-Bit Wired Equivalent Privacy (WEP) Security Support
- 4-Port LAN 10/100Mbps Switch
- 10/100Mbps WAN Port for DSL / Cable Modem
- Support NAT with VPN Passthrough
- Supports MAC/IP/URL Filtering & Domain Blocking

- Supports Scheduling
- Supports DHCP, VPN, PPP, PAP/CHAP
- Single built-in Switch Port can be allocated as DMZ (Demilitarised Zone)
- IEEE 802.1x and WPA, WPA-PSK
- UPnP Enabled
- Single detachable antenna (RP-SMA plug connector)
- Configuration & Management via Web Browser
- Cena bez DPH: 580,-
- Cena s DPH: 690,-

5.1.4 Asus WL-500g Premium

- Datové rozhraní Ethernet, WiFi, USB
- 10/100 Base-T auto-crossover (MDI/MDI-X) Ethernet 4x LAN, 1x WAN
- Další rozhraní 2x USB 2.0
- WiFi standardy IEEE 802.11b/g + Afterburner + BroadRange
- Čipová sada Broadcom
- Provozní režimy Access Point, Home gateway, Router (WiFi režimy: AP/ WDS/ WDS hybrid/ klient)
- WDS/WEP/WPA/WPA2
- RADIUS (802.1x)
- Kontrola přístupů dle MAC (ACL)
- Firewall packetové filtry (LAN -> WAN), URL filtr, SPI, prevence DoS
- NAT (Network Address Translation) Ano (Port Trigger, Virtual Server, DMZ)
- DHCP server, klient - klonování MAC
- Regulace propustnosti dat (QoS) Ano
- VPN (Virtual Private Network) VPN pass through (PPTP, L2TP, IPSec)

- Další síťové služby Bandwidth management, WMM, FTP Server, AiDisk, Print Server, UPnP, NTP client, DDNS klient, Media Server
- CDMA ready
- Management WEB
- Aneténní systém 1 interní / 1 externí (konektor R-SMA)
- Regulace výkonu antény
- Váha a rozměry 500g / 185 x 205 x 36mm
- Cena bez DPH: 1 426,-
- Cena s DPH: 1 698,-

5.1.5 WD My Passport Essential 250GB Externí disk 2.5"

- model WDBAAA2500ABK-EESN
- kapacita 250GB
- rozhraní USB 2.0 (480Mb/s; možno připojit na stávající USB 1.1)
- case odolný proti menším nárazům
- formát disku NTFS
- ochrana přístupu heslem a 256-bit hardwarové šifrování
- kompatibilní s PC (Windows® XP, Windows Vista®, Windows 7) a Mac (Mac OS® X Tiger®, Leopard®, Snow Leopard™)
- rozměry 110 x 15 x 83 mm (d x v x š), hmotnost 200g
- Cena bez DPH: 1 221,-
- Cena s DPH: 1 498,-

5.1.6 HP LaserJet P1005 USB

- Monochromatická laserová tiskárna formátu A4.
- Rychlost tisku až 14 str./min.
- Výstup první stránky do 8 s.

- Standardní paměť 2 MB RAM bez možnosti rozšíření.
- Rozhraní: USB 2.0
- Podporované OS: MS 2000, XP, Vista, Macintosh OS X V10.2.8, V10.3.9, and V10.4.3.
- Doporučené měsíční zatížení: 1.000 stran, maximální 8000 stran.
- Váha 5,2 kg, Rozměry (šířka × hloubka × výška) 347 × 224 × 194 mm
- Spotřební materiál: HP LaserJet CB435A toner / 1500str
- Cena bez DPH: 1 849,-
- Cena s DPH: 2 243,-

5.1.7 Server HP ProLiant ML110 G5 E2160 jako RADIUS + monitor ACER + klávesnice a myš Genius

- Processor(s): One (1) Dual-Core Intel® Pentium® Processor E2160 Processor (1.8GHz, 65W, 800 FSB, 1MB)
- Cache Memory: 1 x 1MB Level 2 cache
- Memory: 1G PC2-6400 ECC (DDR2-800MHz)
- Storage Controller: HP Embedded 6 Port SATA Controller with embedded RAID (4 ports for HDD)
- Hard Drive: 250GB SATA HDD
- Internal Storage: Maximum 2TB (4 x 500GB) SATA
- Optical Drive: 16x SATA DVDRW
- Form Factor: Micro ATX Tower (4U)
- OS Linux Ubuntu 9.10 server
- ACER 17“ LCD V173Bb 1280x1024,7000:1,250cd/m2,5ms
- Genius LuxeMate 300 USB/PS2
- Genius Net Scroll 200 Laser 1600dpi
- Cena bez DPH: 9 084,- + 2330,- + 151,- + 119,- = 11 684,-

- Cena s DPH: 10 824,- + 2 812,- + 180,- + 142,- = 13 958,-

5.1.8 Switch 3COM BaseLine SWITCH 2226 PLUS

- Spravovatelný přes webové rozhraní
- Pracuje na 2. vrstvě
- 24 x 10/100 ports and two dual-purpose Gigabit ports
- Cena bez DPH: 4209,-
- Cena s DPH: 5010,-

5.1.9 Router

Mikrotik Routerboard RB433

- Procesor: Atheros AR7130, 300 MHz
- LAN port: 3 x RJ45 10/100 Mbps MDI/MDI-X
- NAND: 64MB
- Napájení: JACK + POE (16-28 V PoE)
- Ostatní: 1x PC Speaker
- Procesor: MIPS 300 MHz
- Provozní teplota: -20 až 60 °C
- RAM: 64 MB SDRAM
- Rozměry: 15 x 10,5 cm
- Výchozí jméno: admin
- I/O Control: 1x serial port RS-232
- LED indikace: ano
- OS: Mikrotik - RouterOS Level 4
- MiniPCI: 3x miniPCI
- Cena bez DPH: 1503,-

- Cena s DPH: 1789,-

MikroTik R52 miniPCI bezdrátová karta AR5414

- Rozhraní: mini PCI Type III B
- Normy: 802.11a/b/g
- Frekvence: 2.312 – 2.497 GHz (s 5 MHz krokem) a 4.920 – 6.100 GHz (s 5 MHz krokem)
- Chipset: Atheros 5414 s Turbo/Super G
- Konektory: dva U.fl konektory
- Modulace: 802.11a/g: OFDM; 802.11b: CCK (11 Mbps, 5.5 Mbps), DQPSK (2Mbps), DBPSK (1 Mbps)
- Napětí: 3.3V +/- 10% DC; 400mA max (300mA typ.)
- Zabezpečení: 64 and 128 bit WEP; Hardware TKIP and AES-CCM encryption; 802.1x WPA authentication
- Operační systémy: MikroTik RouterOS, Windows XP, Vista, 2000, Linux
- Rozměry: 60mm x 45 mm
- Cena bez DPH: 424,-
- Cena s DPH: 505,-

montážní krabice Mikrotik CA433

- Otvory: 3x RSMA, 1x N female
- Rozměry: 238 x 113 x 30 mm
- Cena bez DPH: 249,-
- Cena s DPH: 296,-

- Celková cena bez DPH: = 2 176,-
- Celková cena s DPH: = 2 590,-

5.1.10 Rack

Eurocase Rack Cabinet GQ5606 6U

- Kapacita: 6U
- šířka: 540mm
- hloubka: 600mm
- výška: 310mm
- Posuvné lišty (rails): Ano
- Otvor pro kabely: horní i dolní kryt
- Umístění: nástěnný i podlahový
- Barevné provedení: černá, povrchová úprava fosfátováním před lakováním
- vnitřní zámek
- Cena bez DPH: 1890,-
- Cena s DPH: 2 249,-

Eurocase Rack Police GA-4-600mm 1U

- Cena bez DPH: 303,-
- Cena s DPH: 361,-

PATCH PANEL 19" S 24 x RJ45 C5

- Cena bez DPH: 639,-
- Cena s DPH: 760,-

- Celková cena bez DPH: 2 832,-
- Celková cena s DPH: 3 370,-

5.1.11 Kabeláž a přípojky

Belden UTP drát Cat 5E

- Barva: Šedá

- Provedení: vnitřní, LSZH (Low Smoke Zero Halogen)
- Kategorie: 5e
- Typ stínění: UTP
- Průřez: AWG 24
- Délka: 305 m
- Provedení kabelu: Drát
- Metráž: Ano
- Cena bez DPH: 1 410,-
- Cena s DPH: 1 678,-

NE KONEKTOR UTP RJ-45 pro drát

- Cena bez,s DPH: 3,-/ks

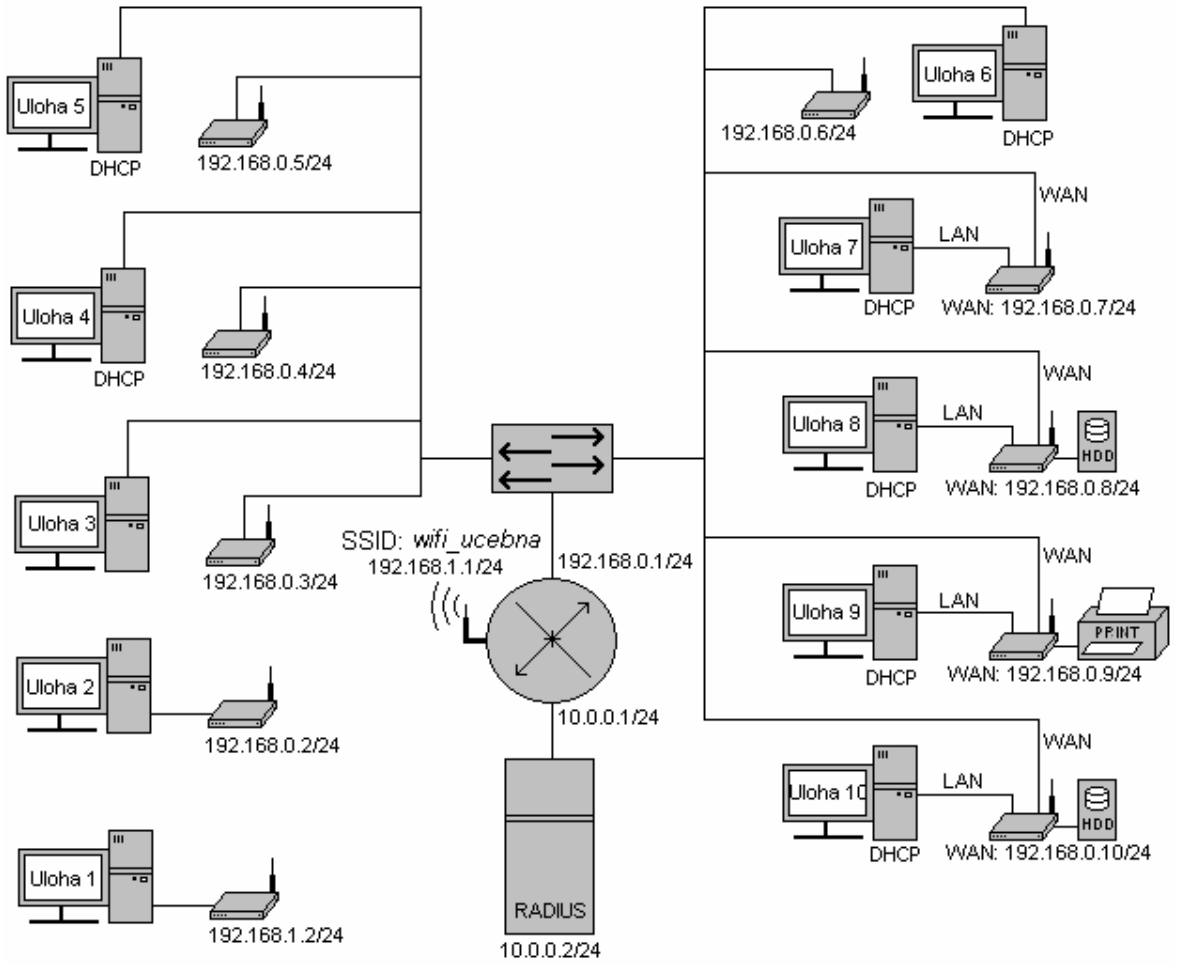
KONEKTOR KRYTKA UTP RJ-45 šedá

- Cena bez DPH: 4,-/ks
- Cena s DPH: 5,-/ks

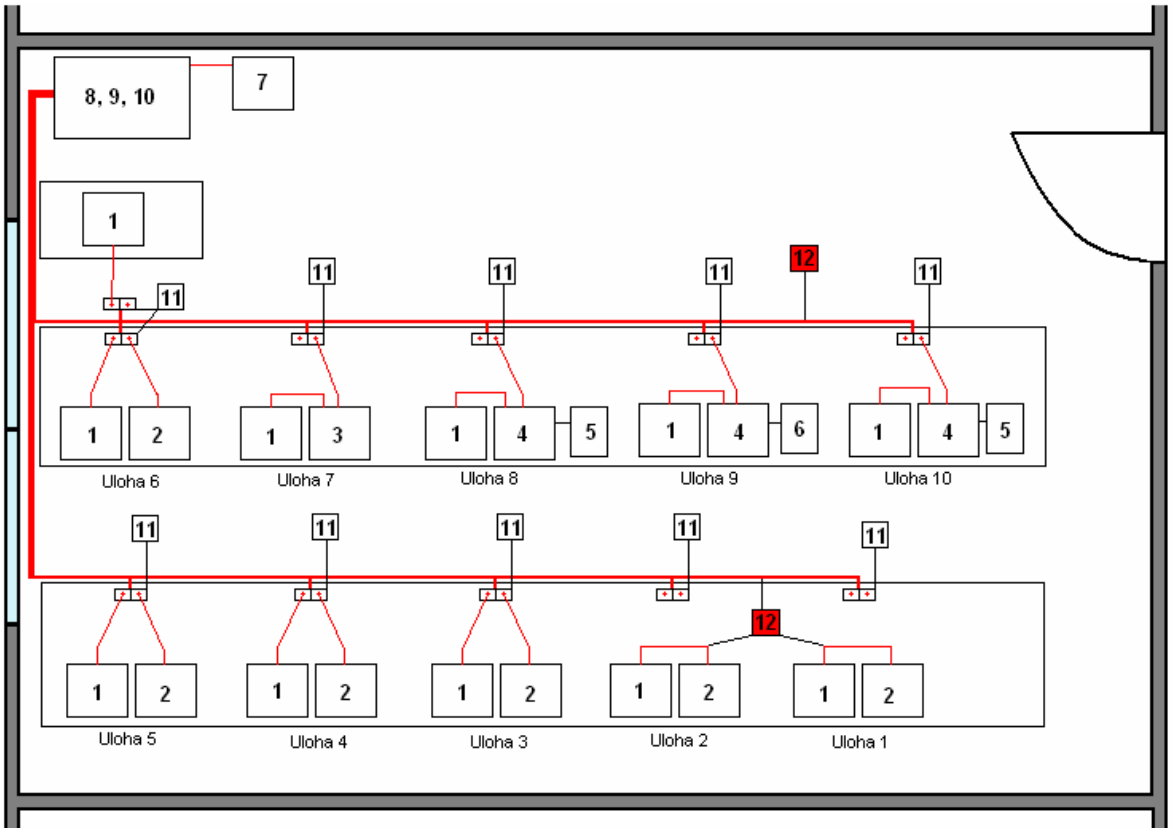
ZÁSUVKA 2x RJ45 NA OMÍTKU

- zásuvka 2x RJ45 na omítku
- narážecí svorky
- barva slonové kosti
- Cena bez DPH: 101,-/ks
- Cena s DPH: 120,-/ks

5.2 Návrh zapojení laboratorní sítě



Obr. 22. Návrh zapojení prvků do sítě



Obr. 23. Blokové schéma učebny

Tab. 3. Seznam použitých zařízení

č.	Artikl	Výrobce	tech.spec	cena bez DPH	cena s DPH
1	PC	Barebone	5.1.1	9 936,00 Kč	11 823,00 Kč
2	Wifi AP	Ovislink	5.1.2	776,00 Kč	924,00 Kč
3	Wifi router 1	D-Link	5.1.3	580,00 Kč	690,00 Kč
4	Wifi router 2	Asus	5.1.4	1 426,00 Kč	1 698,00 Kč
5	Externí HDD	Wester Digital	5.1.5	1 221,00 Kč	1 498,00 Kč
6	Tiskárna	Hewlett-Packard	5.1.6	1 849,00 Kč	2 243,00 Kč
7	Server RADIUS	Hewlett-Packard	5.1.7	11 684,00 Kč	13 958,00 Kč
8	Switch	3Com	5.1.8	4 209,00 Kč	5 010,00 Kč
9	Router	Mikrotik	5.1.9	2 176,00 Kč	2 590,00 Kč
10	Rack	Eurocase	5.1.10	2 832,00 Kč	3 370,00 Kč
11	Síťová zásuvka	Belden	5.1.11	101,00 Kč	120,00 Kč
12	UTB kabel cat. 5e	Belden	5.1.11	1 410,00 Kč	1 678,00 Kč

6 NÁVRH ZADÁNÍ LABORATORNÍCH ÚLOH

6.1 Úloha 1

Přístupový bod OVISLINK 5460 jako klient

- Přes webové rozhraní se připojte k přístupovému bodu OVISLINK 5460:
    - IP adresa zařízení: 192.168.1. 2/24.
    - IP počítače: 192.168.1.x/24.
- Prostudujte si možnosti nastavení, v protokolu uveďte v jakých režimech zařízení může pracovat.
- Nastavte zařízení do módu klient.
- Zjistěte možné dostupné sítě.
- Připojte se k síti „wifi_ucebna“.
- Změňte nastavení protokolu TCP/IP v počítači na získání IP z DHCP.
- Ověřte funkčnost připojení.
- V protokolu uveďte postup při konfiguraci zařízení.
- Jaké informace zařízení poskytuje o nalezených sítích v dosahu?

6.2 Úloha 2

WiFi router OVISLINK 5460, WISP mód (routující klient)

- Přes webové rozhraní se připojte k přístupovému bodu OVISLINK 5460:
    - IP adresa zařízení: 192.168.0.2/24.
    - IP počítače: 192.168.0.x/24.
- Prostudujte si možnosti nastavení..
- Nastavte zařízení do módu WISP (routující klient).
- Nastavte bezdrátové rozhraní a připojte se k síti wifi_ucebna.
- Nastavte LAN rozhraní a server DHCP.
- Změňte nastavení protokolu TCP/IP v počítači na získání IP z DHCP.

- Ověřte funkčnost připojení.
- Jaký je rozdíl mezi módem Klient a WISP ?

6.3 Úloha 3

Přístupový bod OVISLINK 5460 jako AP

- Přes webové rozhraní se připojte k přístupovému bodu OVISLINK 5460:
    - IP adresa zařízení: 192.168.0.3/24.
- Nastavte zařízení do módu AP.
- Nastavte bezdrátové rozhranní, zvolte SSID, vysílací kanál.
- Odpojte váš počítač od sítě LAN, aktivujte bezdrátovou síťovou kartu a připojte se k Vámi vytvořené síti.
- Jaké vysílací kanály Vám toto zařízení nabízí a na jakých frekvencích pracují ?

6.4 Úloha 4

Přístupový bod OVISLINK 5460, základní zabezpečení sítě

- Přes webové rozhraní se připojte k přístupovému bodu OVISLINK 5460:
    - IP adresa zařízení: 192.168.0.4/24.
- Nastavte zařízení do módu AP a vytvořte vlastní síť.
- Prostudujte možnosti zabezpečení bezdrátové sítě pomocí filtru MAC.
- Nastavte filtr MAC adres tak, aby bylo možné přihlásit pouze váš počítač.
- Proveďte zkušební přihlášení k síti.
- Znovu se připojte přes administrační rozhraní k zařízení OVISLINK.
- Prostudujte možnosti zabezpečení pomocí šifrování WEP.
- Proveďte zabezpečení Vaší sítě šifrováním WEP, délku a reprezentaci klíče volte dle vlastního uvážení.
- Připojte se k vámi vytvořené síti.
- Jaké jsou výhody-nevýhody zabezpečení sítě pomocí filtrování MAC adres?

- Jakou šifru využívá Vámi zvolené zabezpečení a jaká je jeho největší slabost.

6.5 Úloha 5

Přístupový bod OVISLINK 5460, pokročilé možnosti zabezpečení pomocí sdíleného klíče

- Přes webové rozhraní se připojte k přístupovému bodu OVISLINK 5460:
    - IP adresa zařízení: 192.168.0.5/24.
- Nastavte zařízení do módu AP a vytvořte vlastní síť.
- Nastavte filtr MAC adres tak, aby bylo možné přihlásit pouze váš počítač.
- Prostudujte možnosti zabezpečení WPA,WPA-2.
- Zvolte metodu šifrování, autentizaci volte pomocí PSK, délku a reprezentaci klíče volte dle vlastního uvážení.
- Připojte se k vámi vytvořené síti.
- Jaké šifrování používá metoda WPA, WPA 2? Jaké jsou největší slabiny této metody zabezpečení sítě?

6.6 Úloha 6

Přístupový bod OVISLINK 5460, pokročilé možnosti zabezpečení pomocí autetizačního serveru RADIUS

- Přes webové rozhraní se připojte k přístupovému bodu OVISLINK 5460:
    - IP adresa zařízení: 192.168.0.6/24.
- Nastavte zařízení do módu AP a vytvořte vlastní síť.
- Nastavte metodu šifrování WPA (TKIP).
- Nastavte autentizaci pomocí serveru RADIUS:
    - IP: 10.0.0.2, Authentication Port: 1812, Accounting Port: 1813, Password: testing123.
- Proveďte nastavení připojení na Vašem počítači:

- Jméno: student, Heslo: student, Šifrování WPA(TKIP), Protokol EAP: PEAP, MS-CHAPv2, bez ověřování certifikátem.

- Připojte se k Vámi vytvořené síti a ověřte funkčnost spojení.
- Jaké jiné možnosti ověření nabízí RADIUS server mimo jména a hesla ?

6.7 Úloha 7

WiFi router D-Link DI-524, nastavení WLAN a LAN, pokročilé zabezpečení WLAN pomocí autentizačního serveru RADIUS

- Přes webové rozhraní se připojte k přístupovému bodu D-Link DL-524, potřebné informace pro připojení zjistěte v nastavení síťového rozhranní:
  - Jméno: admin, Heslo: student.
- Nastavte bezdrátové rozhranní zařízení.
- Nastavte šifrování WPA (TKIP).
- Nastavte autentizaci pomocí serveru RADIUS:
  - IP: 10.0.0.2, Authentication Port: 1812, Password: testing123.
- Nastavte LAN rozhranní a server DHCP.
- Proveďte nastavení připojení na Vašem počítači:
  - Jméno: student, Heslo: student, Šifrování WPA(TKIP), Protokol EAP: PEAP, MS-CHAPv2, bez ověřování certifikátem.
- Připojte se k Vámi vytvořené síti a ověřte funkčnost spojení.

6.8 Úloha 8

WiFi router ASUS WL-500G, nastavení a zabezpečení sítě, nastavení FTP serveru a stažení dat z připojeného USB disku

- Přes webové rozhraní se připojte k přístupovému bodu ASUS WL-500G a seznamte se s jeho administračním rozhranním, potřebné informace pro připojení zjistěte v nastavení síťového rozhranní.

- Vytvořte vlastní bezdrátovou síť a zabezpečte ji (metodu volte dle vlastního uvážení).
- Připojte USB disk k zařízení ASUS a nastavte na zařízení funkci FTP Server
- Připojte se k Vámi vytvořené síti a stáhněte soubor Data/soubor.dat.

6.9 Úloha 9

WiFi router ASUS WL-500G, nastavení a zabezpečení sítě, připojení síťové tiskárny

- Přes webové rozhraní se připojte k přístupovému bodu ASUS WL-500G a seznamte se s jeho administračním rozhranním, potřebné informace pro připojení zjistěte v nastavení síťového rozhranní.
- Vytvořte vlastní bezdrátovou síť a zabezpečte ji (metodu volte dle vlastního uvážení).
- Připojte tiskárnu k USB rozhranní zařízení. Proveďte případná nastavení pro funkci síťové tiskárny na zařízení
- Připojte se k Vámi vytvořené síti, nastavte na počítači síťovou tiskárnu a vytiskněte zkušební stránku.

6.10 Úloha 10

Zhodnocení vlivu šifrování na šířku přenosového pásma

- Přes webové rozhraní se připojte k přístupovému bodu ASUS WL-500G a seznamte se s jeho administračním rozhranním, potřebné informace pro připojení zjistěte v nastavení síťového rozhranní.
- Vytvořte vlastní bezdrátovou síť bez zabezpečení.
- Nastavte na zařízení funkci FTP Server a jako úložiště dat volte připojený USB disk.
- Připojte se k Vámi vytvořené síti.
- Seznamte se s prostředím programu *NetMeter* a nastavte grafické zobrazení dat dle vlastního uvážení.

- Z připojeného FTP disku stáhněte soubor Data/soubor.dat a pomocí programu NetMeter monitorujte rychlost přenosu souboru.
- Znovu se připojte k administračnímu rozhranní přístupového bodu a změňte metodu zabezpečení nejprve na WEP64b,WEP 128b, WPA-PSK, WPA 2-PSK, při každé změně šifrování proveďte stažení souboru a monitoring rychlosti stahování. Porovnejte výsledky jednotlivých měření.
- Porovnejte závislost rychlosti stahování souboru na zvolené metodě zabezpečení, jaký vliv má zvolené zabezpečení na rychlost stahování?

7 ZKUŠEBNÍ REALIZACE PROJEKTU

Aby byla ověřena funkčnost navrženého zapojení v kapitole 5 a proveditelnost laboratorní úlohy navržených v kapitole 6, byla provedena zkušební realizace. Tato realizace byla provedena na dostupných hard-warových prvcích, které se v některých případech neshodují s prvky navrženými výše. Nastavení a zapojeni ovšem u všech prvků probíhá stejným nebo velice podobným způsobem a na vypracováváni jednotlivých laboratorních úloh to nemá vliv.

7.1 Instalace a konfigurace serveru RADIUS

Při zkušební realizaci byla jako první provedena instalace a konfigurace serveru RADIUS. Navrhovaný server HP byl nahrazen sestavou PC AMD Athlon XP 2200, 512 MB DDR, 80GB HDD, na který byl nainstalován OS Ubuntu 9.10 [18]. Po nainstalování OS byl pomocí správce balíčků Synaptic doinstalován server FreeRADIUS 1.1.7 [19], který je dostupný zdarma pod GNU GPL licencí. Jelikož bylo rozhodnuto při konfiguraci využít spojení s databází MySQL, byl doinstalován MySQL server 5.1, MySQL klient 5.1 a phpMyAdmin. Veškeré instalace proběhly bez problému a bylo možné přikročit ke konfiguraci.

Nejprve byla vytvořena databáze radius:

```
mysql –u root –p
     create database radius;
     exit
```

Dále byla vytvořena struktura databáze radius. Pro vytvoření bylo využito konfiguračního souboru `mysql.sql`, který je umístěn v adresáři instalačního balíčku serveru freeradius:

```
cd /freeradius-1.1.7/doc/examples/
     mysql –uroot –psql123 radius < mysql.sql
```

Jako poslední bylo třeba nastavit v souboru `/etc/mysql/my.cnf` , aby MySQL server poslouchal na všech rozhranních, ne jen na loopbacku. Stačilo zakomentovat řádek `bind-address = 127.0.0.1` (Obr. 24).

```
#
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
#bind-address           = 127.0.0.1
```

Obr. 24. Editovaný řádek v souboru my.cnf

Tím je databáze MySQL nastavena. Záznamy do tabulek budou popsány později.

Dále je třeba upravit několik konfiguračních souborů serveru radius ve složce `etc/freeradius`. Jako první byl konfigurován soubor `sql.conf`. V sekci CONNECT bylo třeba nastavit logovací údaje k databázi (Obr. 25).

```
# Connect info
server = "localhost"
login = "root"
password = "sql123"
```

Obr. 25. Connect info v souboru sql.conf

Dále bylo třeba úplně na konci souboru odkomentovat řádek `#radclients = yes` (Obr. 26). Tím bylo nastaveno, že server bude klienty číst z tabulky NAS v databázi radius a ne ze souboru `clients.conf`.

```
#
# Set to 'yes' to read radius clients from the database ('nas' table)
readclients = yes
```

Obr. 26. Editovaný řádek v soboru sql.conf

Jako další bylo třeba nastavit hlavní konfigurační soubor radius serveru, `radiusd.conf`. Nejprve bylo třeba nastavit IP adresu, na které bude server poslouchat (Obr. 27).

```
#  bind_address:  Make the server listen on a particular IP address, and
#  send replies out from that address.  This directive is most useful
#  for machines with multiple IP addresses on one interface.
#
#  It can either contain "*", or an IP address, or a fully qualified
#  Internet domain name.  The default is "*"
#
#  As of 1.0, you can also use the "listen" directive.  See below for
#  more information.
#
bind_address = 10.0.0.2
```

Obr. 27. Editovaný řádek bind_address v souboru radiusd.conf

Dále pak v sekci `authorize{}` zakomentovat řádek `files` a odkomentovat řádek `#sql` (Obr. 28).

```
        #  Read the 'users' file
#       files

        #
        #  Look in an SQL database.  The schema of the database
        #  is meant to mirror the "users" file.
        #
        #  See "Authorization Queries" in sql.conf
        sql
```

Obr. 28. Editovaná sekce auhorize {} v souboru radiusd.conf

V sekci `authenticate{}` zakomentovat řádek `unix` (Obr. 29).

```
        #  See 'man getpwent' for information on how the 'unix'
        #  module checks the users password.  Note that packets
        #  containing CHAP-Password attributes CANNOT be authenticated
        #  against /etc/passwd!  See the FAQ for details.
        #
#       unix
```

Obr. 29. Editovaná sekce authenticat{} v souboru radiusd.conf

V sekci `preacct{}` zakomentovat řádek `files` (Obr. 30).

```
        #
        #  Read the 'acct_users' file
#       files
```

Obr. 30. Editovaná sekce preacct{} v souboru radiusd.conf

V sekci `accounting{}` zakomentovat řádek `unix`, zakomentovat `radutmp` a odkomentovat `#sql` (Obr. 31).

```
        #  Update the wtmp file
        #
        #  If you don't use "radlast", you can delete this line.
#       unix

        #
        #  For Simultaneous-Use tracking.
        #
        #  Due to packet losses in the network, the data here
        #  may be incorrect.  There is little we can do about it.
#       radutmp
#       sradutmp

        #  Return an address to the IP Pool when we see a stop record.
#       main_pool
#       sqlippool

        #
        #  Log traffic to an SQL database.
        #
        #  See "Accounting queries" in sql.conf
        sql
```

Obr. 31. Editovaná sekce accounting{} v souboru radiusd.conf

V sekci `postauth{}` odkomentuju `#sql` (Obr. 32).

```
        #
        #  See "Authentication Logging Queries" in sql.conf
        sql
```

Obr. 32. Editovaná sekce postauth{} v souboru radiusd.conf

Jako poslední byla provedena editace souboru eap.conf, kde je uloženo nastavení jednotlivých bezpečnostním protokolů radius serveru. Zde byla adkomentována sekce *peap{}* (Obr.33).

```
peap {
        default_eap_type = mschapv2
        copy_request_to_tunnel = no
        use_tunneled_reply = no
        proxy_tunneled_request_as_eap = yes
}
```

Obr. 33. Editovaná sekce peap{} v souboru eap.conf

Tím byla veškerá konfigurace RADIUS serveru provedena. Pro plnou funkčnost bylo ještě třeba naplnit tabulky v mysql databází radius. Jako první byl proveden zápis do tabulky *nas*. V této tabulce jsou uvedeni klienti, kteří poskytují služby RADIUS serveru. Do tabulky byly zadány následující údaje:

```
ID = „“
nasname = „192.168.0.0/24“
shortname= „wifi_ap“
type=„other“
ports= „null“
secret= „testing123“
community= „null“
description= „RADIUS Client“
```

Tyto údaje byly zadány z příkazové řádky příkazem:

```
INSERT INTO `nas` VALUES ('', '192.168.0.0/24', 'wifi_ap',
'other', null, 'testing123', null, 'RADIUS Client');
```

Jako *nasname* bylo zadáno číslo sítě, aby server akceptoval jakékoli zařízení zapojené v sítí. Je možné zadávat i přímo jednotlivá zařízení, v takovém případě je nutné jako *nasname* uvádět přímo IP adresu takového zařízení.

Jako poslední byly v tabulce *radcheck* vytvořeny logovací údaje pro uživatele s parametry:

```
ID= „“
UserName= „student“
Attribute= „Cleartext-Password“
op= „:=“
Value= „student“
```

Tyto údaje byly zadány z příkazové řádky příkazem:

```
INSERT INTO `radcheck` VALUES ('', 'student', 'Cleartext-
Password', ':=', 'student');
```

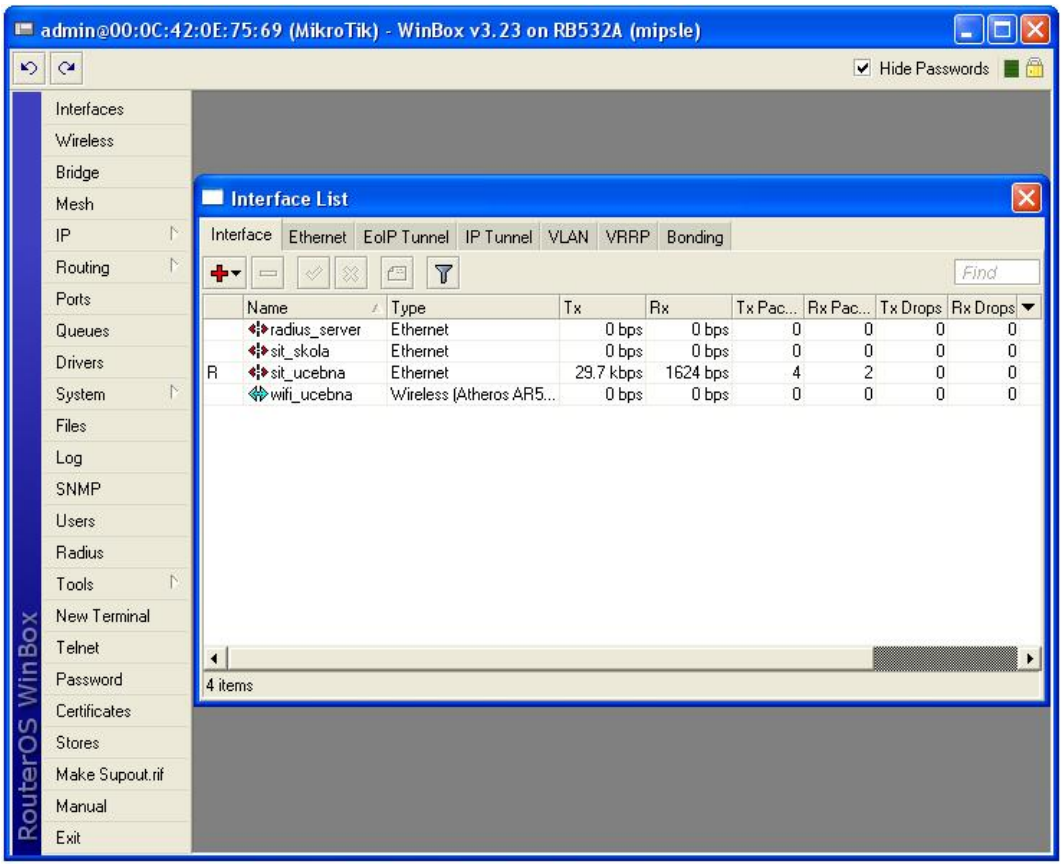
Po provedení těchto změn byl RADIUS server nastaven a může být spuštěn. Pokud je server spuštěn v debug módu příkazem `sudo freeradius -X`, je možné sledovat odpovědi serveru a následně pak doladit případné chyby.

Kompletní konfigurační soubory jsou uloženy na CD, viz příloha č. P II.

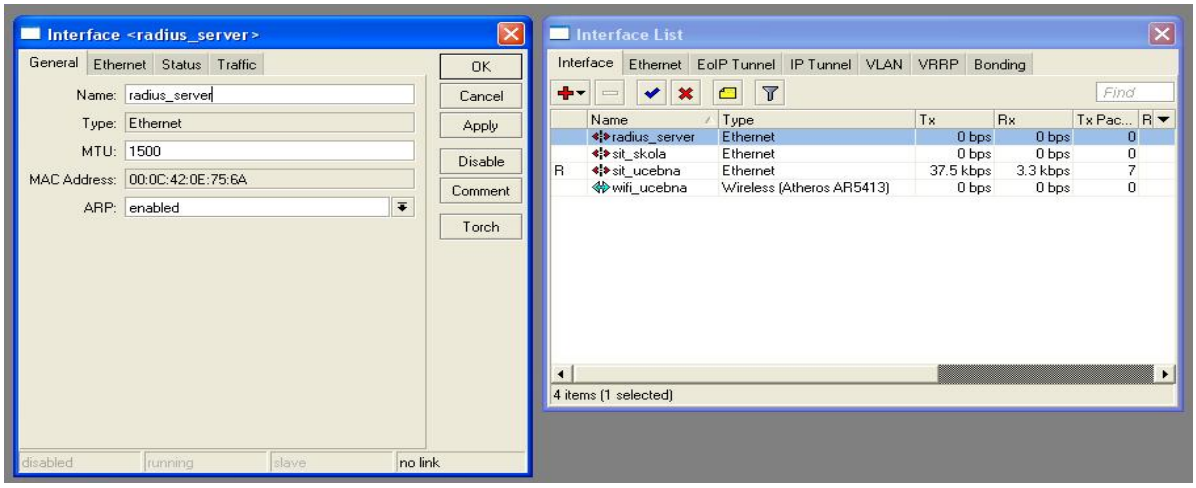
7.2 Konfigurace RouterBoardu Mikrotik

Jako další bylo provedeno nastavení Routerboardu Mikrotik. Navrhovaný Mikrotik RB 433 + Wifi miniPCI karta Mikrotik R52 byl nahrazen dostupným RB532A se stejnou miniPCI wifi kartou. Použitý routerboard je, stejně jako navržený, osazen 3 LAN porty, 2 porty MiniPCI a má nainstalován operační systém RouterOS v 2.9.23, lyší se pouze rychlejším procesorem o taktu 400MHz.

Editace routerboardu byla provedena pomocí programu WinBox 2.2.10. Nejprve bylo provedeno pojmenování jednotlivých rozhranní pro lepší přehlednost při další konfiguraci `Interface-> Interface List` (Obr. 35).

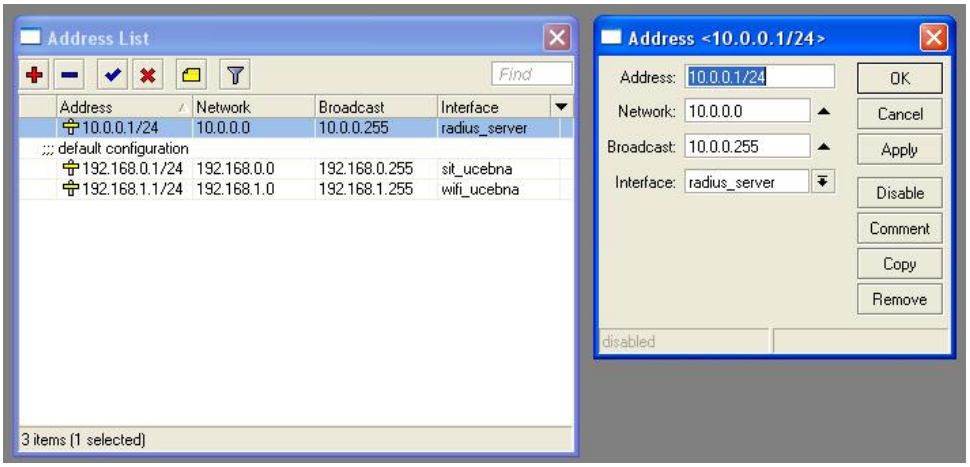


Obr. 34. Pracovní prostředí programu WinBox



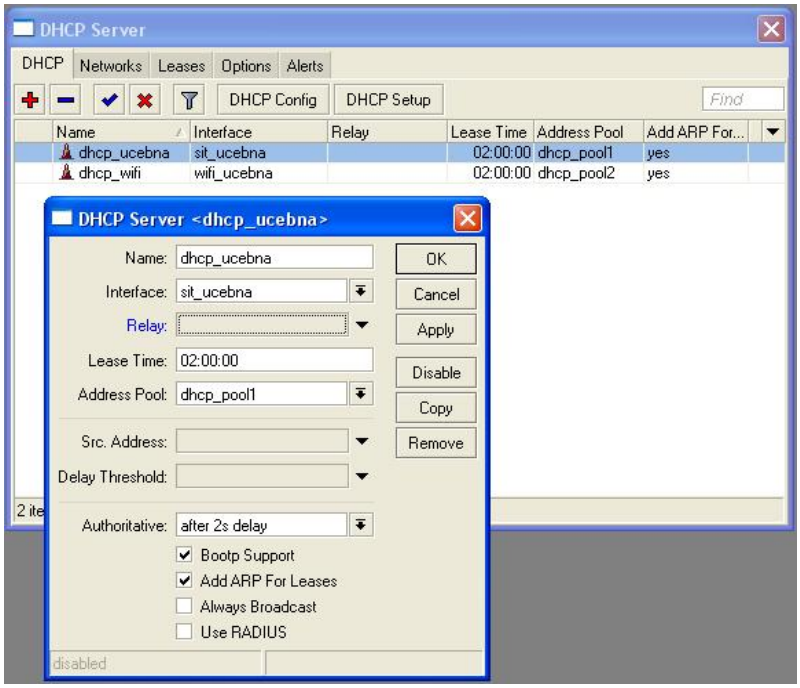
Obr. 35. Přejmenování jednotlivých rozhraní routerboardu Mikrotik

Jako další bylo provedeno přiřazení sítí k jednotlivým rozhranním `IP-> Address List` (Obr. 36), tak jak to bylo navrženo v kapitole 5.2.



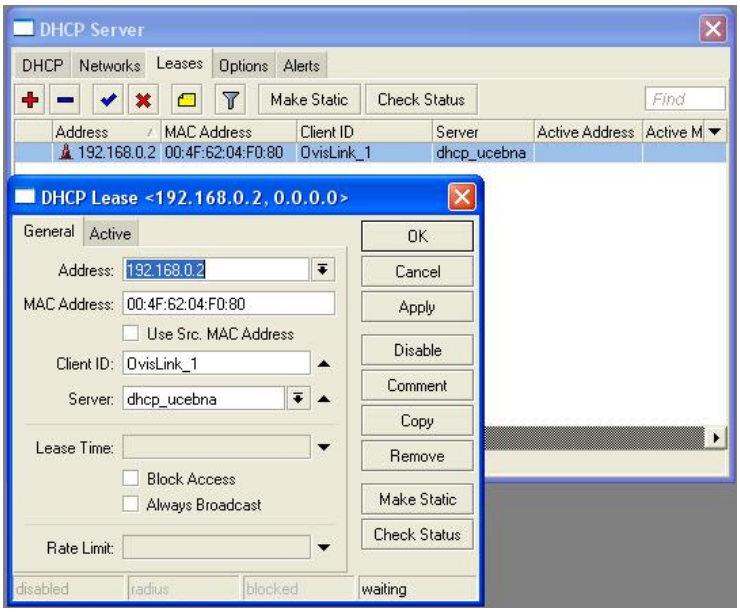
Obr. 36. Přiřazení jednotlivých sítí k rozhranním routerboardu Mikrotik

Jakmile byla nastavena jednotlivá rozhranní, bylo provedeno nastavení serveru DHCP, *IP-> DHCP server*, (Obr. 37). V závorce je vždy uvedena hodnota nastavovaná pro síť učebny. Přes menu DHCP setup bylo nastaveno nejprve rozhranní (sit_ucebna), poté síť, do které bude DHCP server přiřazen (192.168.0.0/24), brána DHCP serveru (192.168.0.1), rozsah přiřazovaných adres (192.168.0.2 – 192.168.0.50) a dobu propůjčení IP adresy (03:00:00). Stejným způsobem byl nastaven DHCP server i pro wifi rozhranní.



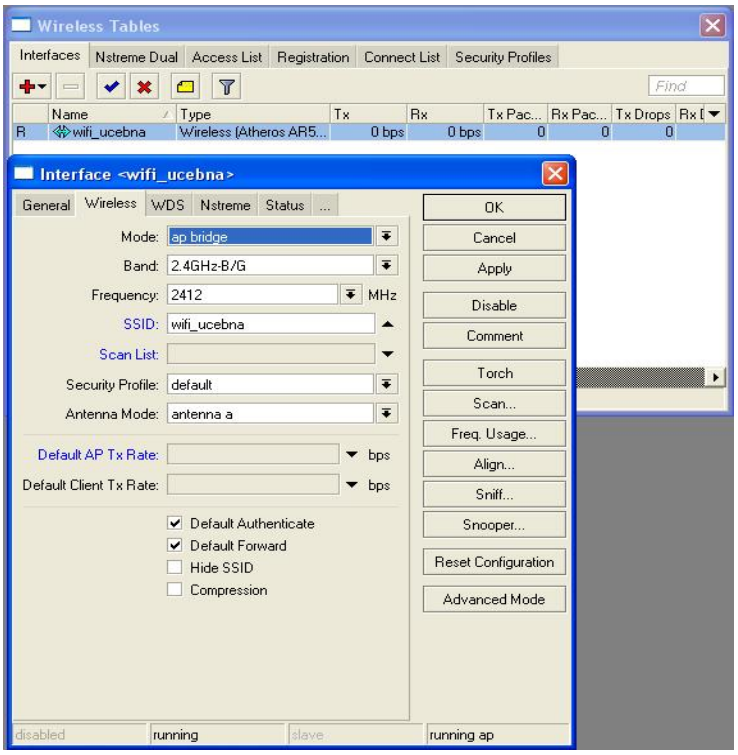
Obr. 37. Nastavené DHCP servery v zařízení Mikrotik

Aby bylo zaručeno, že jednotlivé bezdrátové prvky, určené k výuce, budou mít přiřazeny vždy stejné předem určené adresy, je třeba v záložce `Leases` přednastavit jednotlivé statické klienty. IP adresy jim budou přiřazeny podle MAC adresy (Obr. 38).



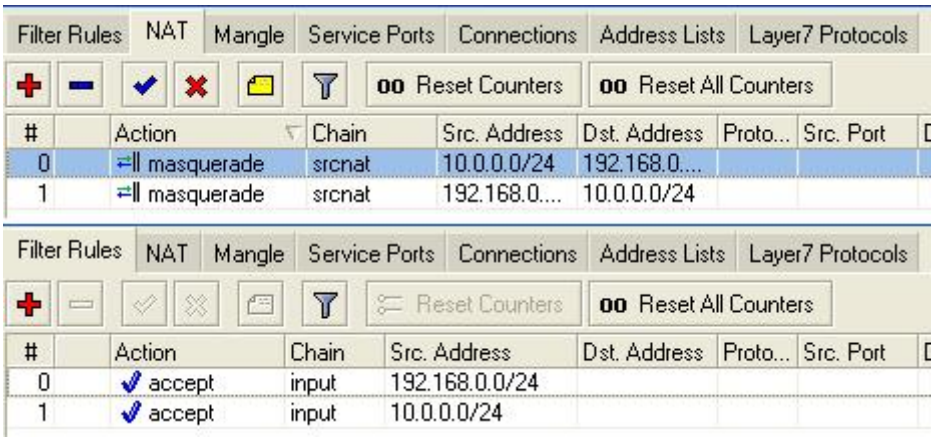
Obr. 38. Nastavení statických klientů serveru DHCP na routerboardu Mikrotik

Tím byla nastavena všechna LAN rozhranní a dále bylo provedeno nastavení wifi rozhraní do režimu přístupového bodu, menu `Wireless`, (Obr. 39).



Obr. 39. Nastavení wifi rozhraní routerboardu Mikrotik

Tím byla nastavena všechna rozhranní a jednotlivé sítě jsou samostatně funkční, ovšem aby byl umožněn provoz mezi sítěmi, bylo třeba nastavit ještě pravidla provozu a NAT, *IP->Firewall*, (Obr. 40).



Obr. 40. Nastavení pravidel a NAT

Provedené nastavení bylo uloženo do souboru *MikroTik.backup* a je uloženo na přiloženém CD, viz. příloha č. P II.

7.3 Tvorba zkušebních protokolů

Po zapojení testovací sítě bylo provedeno vypracování protokolů přesně podle jednotlivých zadání, uvedených v kapitole 6. Jednotlivé protokoly jsou uvedeny v příloze číslo P I.

Po vypracování každého zadání bylo nastavení bezdrátového prvku uloženo do souboru. Jednotlivé soubory jsou uloženy na přiloženém CD viz. příloha č. P II. Funkčnost jednotlivých zapojení tedy lze kdykoli ověřit nahráním uloženého nastavení do příslušného zařízení.

8 TUTORIÁL K ZAŘÍZENÍ OVISLINK WL-5460

Jako výuková pomůcka byl vytvořen tutoriál k zařízení OvisLink WL-5460 v programu Wink.

Tutoriál je rozdělen do čtyř základních částí :

1. část – Popis zařízení OvisLink WL-5460AP
2. část - Připojení k zařízení a popis pracovních režimů.
3. část – Nastavení zařízení do režimu AP včetně zabezpečení.
4. část – Nastavení zařízení do režimu Klient.
5. část – Nastavení zařízení do režimu WISP.

Na úvodní stránce tutoriálu bude rozcestník, který uživateli umožní zvolit si jednu z částí tutoriálu. Po projetí celé části bude uživatel vrácen zpět na úvodní stránku.

Hotový tutoriál byl vyexportován ve třech formátech, exe soubor, flash animace a dokument pdf. Všechny výstupní soubory jsou uloženy na CD, viz. příloha číslo P II.

8.1 Program WINK

Wink je program určený k vytváření návodů a prezentací, původně pro vytváření návodů, jak používat software (například pro MS-Word/Excel atd). Pomocí Winku můžete pořizovat snímky obrazovky s vaším software, můžete použít obrázky, které už máte připravené, napsat vysvětlivky pro každý krok, vytvořit sekvence s navigací, tlačítky, pauzami, titulky a podobně a tak vytvořit efektivní návody pro vaše uživatele.

Základními vlastnostmi programu WINK jsou:

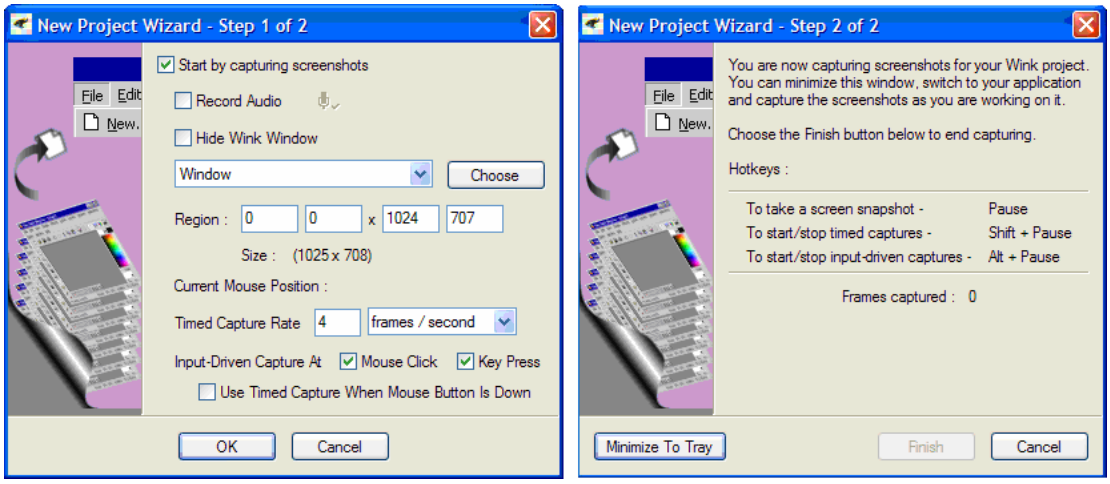
- **Freeware:** Wink je freeware pro komerční i osobní užití. V případě, že byste jej chtěli dále distribuovat, potřebujete souhlas autora .
- **Smart Capture Tools:** Snímá obrazovky automaticky tak, jak používáte PC na zákadě na práce s myší a klávesnicí (šetří čas a vytváří profesionální snímky).
- **Vstupní formáty:** Zachytává snímky obrazovky vašeho PC nebo používá obrázky ve formátech BMP/JPG/PNG/TIFF/GIF.

- **Výstupní formáty:** Export jako Macromedia Flash, Standalone EXE (spustitelný soubor), PDF, PostScript, HTML nebo výše uvedené formáty obrázků. Flash/html použijete na webu, EXE pro distribuci uživatelům PC a PDF pro manuály k tisku.
- **Podpora jazyků:** Angličtina, francouzština, němčina, italština, dánština, brazilská portugalština a zjednodušená/tradiční čínština.
- **Nástroje:**
    - Navigační tlačítka pro pohyb na následující/předchozí/náhodný snímek v prezentaci, můžete použít vlastní obrázky pro tato tlačítka (plná podpora pro průhlednost/alfa kanál).
    - Popisy a bubliny pro zobrazení vysvětlivek. Zabudovaným editorem můžete vytvořit své vlastní tvary popisů.
    - Intuitivní editace snímků, popisků, kerzorů, navigačních tlačítek a titulků pomocí drag-n-drop.
    - Rozšířené vlastnosti jako šablony, editace kurzorů, palet, pozadí, ovládání a preloaderu pro flash atd.
    - Kompletní podpora PC a webu s exportem do PDF, HTML, SWF a EXE.
    - Použitím inovativní kompresní techniky je zmenšena velikost výstupních souborů Flash. Vygenerované soubory se dají přehrát ve Flash player od verze 3 výše.

[20]

8.2 Práce s programem WINK při tvorbě tutoriálu

Nejprve byl v programu vytvořen nový projekt a bylo třeba nastavit základní parametry (Obr. 41.).



Obr. 41. Vytvoření Nového projektu ve WINK, krok 1 a 2

Funkce jednotlivých nabízených klávesových zkratek :

`Pause` - Pořídí jeden screenshot.

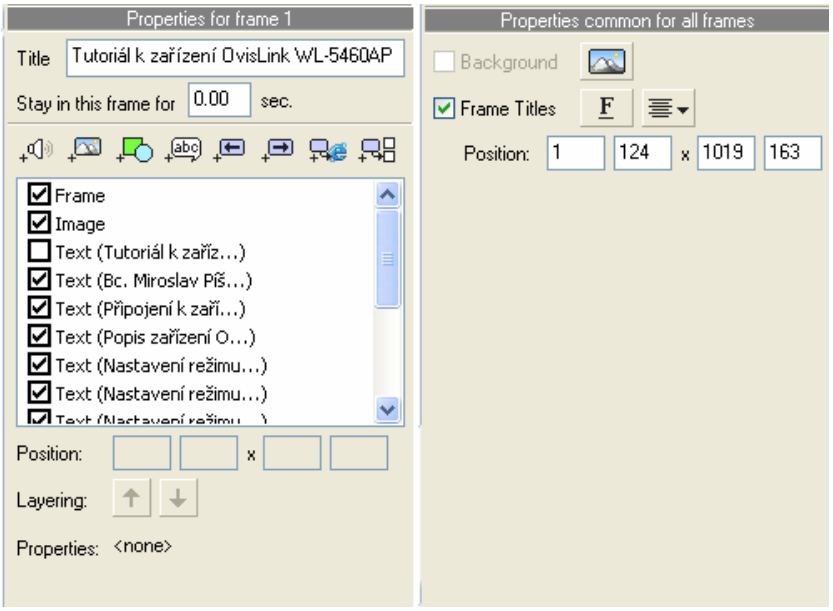
`Shift+Pause` - Spustí a zastaví záznam screenshotů.

`Alt+Pause` - Spustí input-driven záznam.

Po kliknutí na tlačítko **`Finish`** ukončíme záznam a pořízené screenshoty se nahrají do programu, kde s nimi můžeme dál pracovat a vytvářet samotný tutoriál nebo již uvedenými kl. zkratkami pokračovat v pořizování screenshotů.

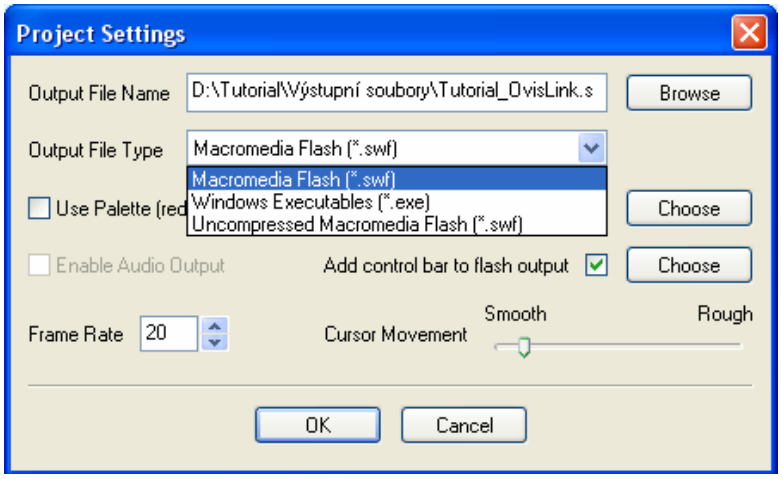
Obr. 42. Pracovní prostředí programu WINK

Ve spodní části pracovního prostředí jsou umístěny jednotlivé pořízené screenshoty. Ty byly postupně zpracovávány. Z tabulky *Properties* na pravé straně obrazovky do nich byly vkládány navigační tlačítka, textová pole a jiné grafické prvky.



Obr. 43. Tabulka Properties framu č. 1

Hotový tutoriál lze vyexportovat do výstupních soborů pomocí tlačítka *Render* v horní liště programu. Před samotným exportem je třeba ještě nastavit atributy výstupního formátu (Obr. 44), tlačítko *Project Settings*.



Obr. 44. Nastavení vlastností výstupního souboru programu WINK

Z výstupních souborů je k dispozici Flash, exe soubor a nekomprimovaný Flash. Po provedení nastavení změny uložíme tlačítkem OK. Výstupní soubor se uloží na zvolené místo.

ZÁVĚR

Bezdrátové wifi sítě se v posledních několika letech dočkaly velkého rozmachu a můžeme se s nimi setkat doslova na každém kroku. Jejich znalost se pro absolventa oboru Informačních technologií stává doslova nutností. Proto si tato práce kladla za cíl navrhnout laboratoř pro výuku bezdrátových wifi sítí jak po stránce jednotlivých síťových komponentů a jejich zapojení, tak i samotných laboratorních úloh.

Teoretická část této práce se věnuje obecné problematice bezdrátových wifi síť. První kapitola definuje pojem bezdrátová wifi síť, jednotlivé její standardy, frekvenční spektrum, komponenty sítě a architekturu jejich zapojení. V druhé kapitole jsou uvedeny jednotlivé možnosti zabezpečení wifi sítí od těch nejjednodušších a až po ty nejdokonalejší. Poslední kapitola teoretické části se pak věnuje jednotlivým hard-warovým prvkům využívaným při realizaci..

Praktická část pak obsahuje samotný návrh laboratoře. První kapitola praktické části hodnotí současný stav praktické výuky nejen wifi sítí na Fakultě Aplikované Informatiky, UTB ve Zlíně a odůvodňuje tak případnou realizaci tohoto návrhu. Druhá kapitola praktické části obsahuje detailní popis navrhovaných hardwarových prvků, jejich zapojení v laboratoři a jednoduchou kalkulaci nákladů na jejich nákup. Další kapitola obsahuje návrh zadání celkem 10 laboratorních úloh.

Aby byla ověřena funkčnost navrženého zapojení a proveditelnost jednotlivých laboratorních úloh, bylo provedeno zkušební zapojení celé sítě a následné vypracování navržených laboratorních úloh a příslušných protokolů. Popis této realizace je uveden v poslední kapitole této práce.

Jako pomůcka pro výuku byl také vytvořen tutoriál, který podrobně popisuje práci s vybraným bezdrátovým přístupovým bodem OvislLink WL-5460 a jeho nastavení do základních pracovních módů.

Pokud by došlo alespoň k částečné realizaci tohoto projektu a jeho následnému zavedení do výuky, studenti by získaly praktické zkušenosti s administrací bezdrátových síťových prvků. Dokázaly by bezdrátovou síť nejen vytvořit ale také jí patřičně zabezpečit a to s pomocí jakéhokoli bezdrátového zařízení na trhu.

CONCLUSION

In the last few years there was a big development of wireless network and we can see it everywhere. Knowledge about it is going to be necessary for a graduate in the field of Information Technology. That is why this work should show a design of a laboratory for teaching about wireless network, about their components and connection and also doing laboratory exercises.

The theoretical part of this work deals with general questions about wireless network. The first chapter defines a conception of wireless network, standards in using, frequency spectrum, components of network and structure of connection. In the second chapter there are mentioned basic and also master possibilities of securing wifi. The last chapter deals with single hard-ware parts which are used for realization.

The practical part contains the design of the laboratory itself. The first chapter of the practical part evaluates the contemporary condition of practical teaching of wifi at Faculty of Informatics, UTB in Zlin and also speaks about realization of this design. The second chapter of the practical part contains detailed description of hard-ware parts, their integration in the laboratory and a simple calculation of charges for their purchasing. The next chapter contains a project of 10 laboratory exercises.

Because of testing of the designed connection and the function of the exercises, a trial connection of the whole network and also elaboration of every task and appropriate protocols were made.

A tutorial was also prepared as a device for teaching, which describes the work with wireless access point Ovis1Link WL-5460 and its configuration into general work modes.

If this project was at least partially realized and consequently used in teaching, students would gain practical experience in work with wireless network issues. They would be able to create network and also create capable security of the network with any kind of device in the world market.

SEZNAM POUŽITÉ LITERATURY

[1] BARKEN, Lee. *Jak zabezpečit bezdrátovou síť Wi-Fi*. Jiří Veselský. 1. vyd. Brno : Computer Press, 2004. 176 s. ISBN 80-251-0346-3.

[2] PUŽMOVÁ, Rita. *Bezpečnost bezdrátové komunikace : Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G*. 1. vyd. Brno : Computer Press, 2005. 184 s. ISBN 80-251-0791-4.

[3] ZANDL, Patrick. *Bezdrátové sítě Wi-Fi : Praktický průvodce*. 1. vyd. Brno : Computer Press, 2003. 204 s. ISBN 80-7226-632-2.

[4] KÖHRE, Thomas. *Stavíme si bezdrátovou síť Wi-fi*. Marek Šiller. 1. vyd. Brno : Computer Press, 2004. 296 s. ISBN 80-251-0391-9.

[5] BRISBIN, Shelly. *Wi-Fi – postavte si svou vlastní wi-fi síť*. 1. vyd. Praha : Neocortex, 2004. 239 s. ISBN 80-86330-13-3.

[6] HORÁK, Jaroslav. *Malá počítačová síť doma a ve firmě*. 1. vyd. Praha : Grada, 2003. 183 s. ISBN 80-24705-82-6.

[7] TRULOVE, James. *Sítě LAN : hardware, instalace a zapojení*. Tomáš Znamenáček. 1. vyd. Praha : Grada, 2009. 384 s. ISBN 978-80-247-2098-2.

[8] DAVIS, Harold. *Bezdrátové sítě Wi-Fi : Průvodceúplného začátečníka*. Karel Voráček. 1. vyd. Praha : Grada Publishing, 2006. 376 s. ISBN 80-247-1391-8.

[9] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. David Krásenský. 1. vyd. Brno : Computer Press, 2005. 344 s. ISBN 80-251-0417-6.

[10] Svět sítí [online]. c2000-2010 [cit. 2010-04-10]. Dostupný z WWW: <http://svetsiti.cz/>.

[11] ŘEHÁK, Jan. Co je to WiFi : úvod do technologie. *Hw.cz* [online]. 2003 [cit. 2010-03-18]. Dostupný z WWW: <http://hw.cz/Produkty/Ethernet/ART915-Co-je-to-WiFi---uvod-do-technologie.html>.

[12] *IEEE CS : Československá sekce IEEE* [online]. 22.3.2010 [cit. 2010-03-22]. Dostupný z WWW: <http://www.ieee.cz/>.

[13] *IEEE 802 :IEEE 802 LAN/MAN Standards Committee* [online]. [2000] , 25.2.2010 [cit. 2008-03-01]. Angličtina. Dostupný z WWW: <http://www.ieee802.org/>.

[14] REMER, Jiří. Mobilní technologie v českých organizacích. *Mobile & Wireless Solutions* [online]. 2007 [cit. 2010-03-03]. Dostupný z WWW: <http://www.mobilewireless.cz/files/Remr_MWS07.pdf>.

[15] IEEE 802.11. *Wikipedie : otevřená encyklopedie* [online]. 2008 [cit. 2010-03-20]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/IEEE_802.11>.

[16] PRAVDA, Ivan. Přehled doplňků standardu IEEE 802.11. *Access server* [online]. 2005 [cit. 2010-03-03]. Dostupný z WWW: <http://access.feld.cvut.cz/view.php?nazevclanku=&cisloclanku=2005113002>.

[17] PETERKA, Jiří. Báječný svět počítačových sítí : seriál, PC World. *E-archiv : archiv článků a přednášek Jiřího Peterky* [online]. 2005-2007 [cit. 2010-03-15]. Dostupný z WWW: <http://www.earchiv.cz/i_bajecnysvet.php3>.

[18] *Ubuntu* [online]. c2007-2010 [cit. 2010-03-21]. Dostupné z WWW: <www.ubuntu.cz>.

[19] *FreeRADIUS* [online]. 2009, 30.12.2009 [cit. 2010-04-11]. Dostupné z WWW: <http://freeradius.org/>.

[20] *DebugMode WINK*[online]. c2010 [cit. 2010-04-15]. Dostupné z WWW: http://www.debugmode.com/wink/.

[21] Protokol PEAP. *MicrosoftTechNet : Microsoft Windows Server TechCenter* [online]. 2005 [cit. 2010-05-30]. Dostupný z WWW: <http://technet2.microsoft.com/windowsserver/cs/library/3e94a25d-8922-4935-b248-540aa6b8c5101029.mspx?mfr=true>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES	Advanced Encryption Standard
AP	Acccess Point
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
CBC	Cipher Block Chaining
CCMP	Counter mode - CBC Message authentication Protocol
CRC	Cyclic Redundancy Check
dB	Decibel
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DSL	Digital Subscribe Line
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol Over LAN's
EAP-TLS	EAP - Transport Layer Security
EAP-TTLS	EAP - Tunneled Transport Layer Security
EIRP	Equivalent Isotropically Radiated Power
ESS	Extended Service Set
ESSID	Extended Service Set IDentifier
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
GNU GPL	GNU General Public License
HDD	Hard Disk Drive
HTTP	HyperText Transport Protocol
CHAP	Challenge Authentication Protocol
IEEE	Institute of Electrical and Electronics Engineers

IAPP	Inter-Access Point Protocol
IV	Initialization Vector
MAC	Media Access Control
MAC	Message Authentication Code
MD5	Message Digest
MIC	Message Integrity Check
MPDU	Mac Protocol Data Unit
MsCHAP	Microsoft Challenge-Handshake Authentication Protocol
MySQL	My Select Query Language
PDA	Persondal Digital Assistant
PKI	Publik Key Infrastructure
PMK	Pairwise Master Key
PN	Packet Number
PPP	Point to Point Protocol
PSK	Pre-Shared Key
QoS	Quality Of Service
RADIUS	Remote Authentication Dial-In User Service
RC4	Ron's Code No. 4
TK	Temporary Key
TKIP	Temporal Key Integrity Protocol
TMK	Temporary MIC Key
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

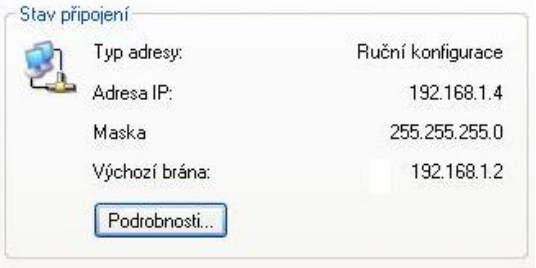
SEZNAM PŘÍLOH

PŘÍLOHA P I: VYPRACOVANÉ VZOROVÉ PROTOKOLY

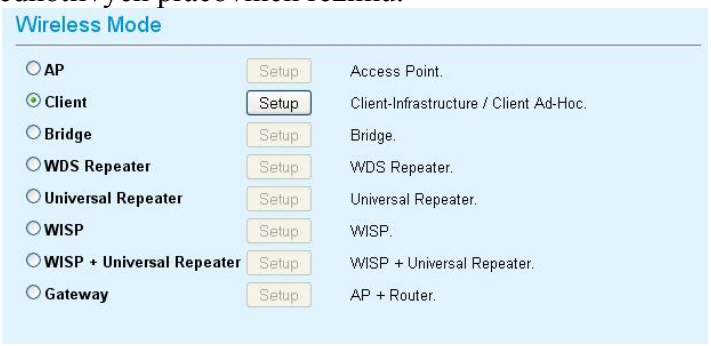
Univerzita Tomáše Bati ve Zlíně Fakulta aplikované informatiky	
Vypracoval: Bc. Miroslav PÍŠA	Ročník / Skupina:
Předmět: **Zkušební realizace Diplomové práce**	Datum:
Úloha: **1. Přístupový bod OVISLINK 5460 jako klient**	Hodnocení:

1 Vypracování

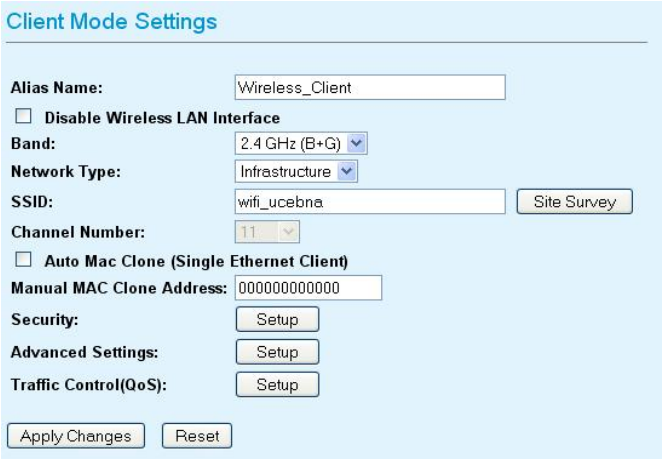
Byla provedena ruční konfigurace síťového rozhraní na PC podle zadání.



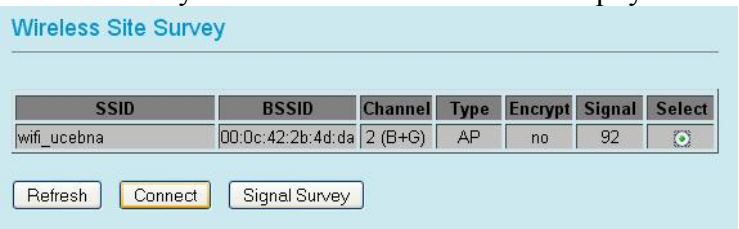
Pomocí webového prohlížeče jsem se připojil ke konfiguračnímu rozhraní zařízení. Na úvodní stránce je nabídka jednotlivých pracovních režimů.



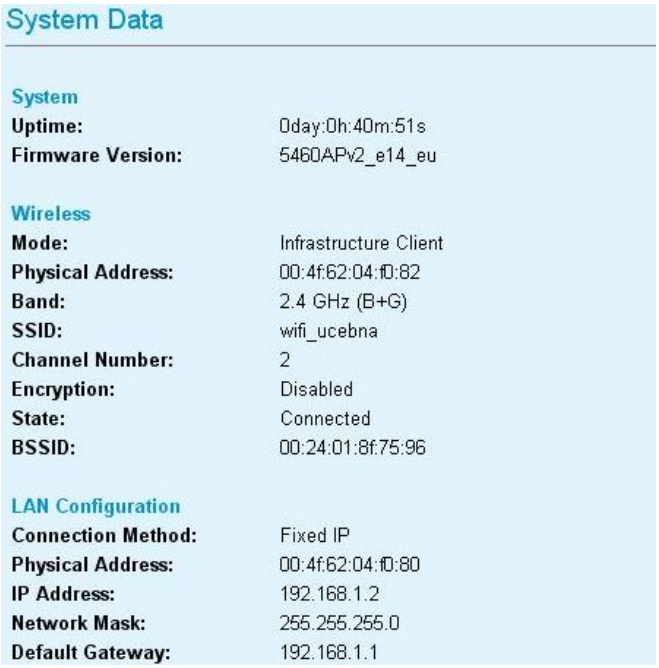
Vybral jsem mód klient a přes tlačítko Setup jsem se dostal ke konfiguraci tohoto pracovního režimu. Pro mód klienta bylo třeba nastavit pouze frekvenční pásmo ve kterém bude klient pracovat. V tomhle případě tedy 2.4GHz (B+G). Dále pak typ sítě ke které se bude zařízení připojovat, tedy infrastrukture.



Kliknutím na tlačítko Site Survey se se dostal na zobrazení dostupných sítí.



V dosahu byla pouze jedna síť, wifi_ucebna, pro připojení k ní bylo třeba ji označit v kolonce Select a pak kliknout na tlačítko Connect. Jelikož bylo připojení k síti úspěšné, objevila se zpráva „Connect successfully!“. Tlačítkem OK jsem se vrátil zpět na nastavení, které již není třeba dále editovat. V horním menu se po kliknutí na tlačítko Status->System Data se zobrazí kompletní informace o aktuálním nastavení

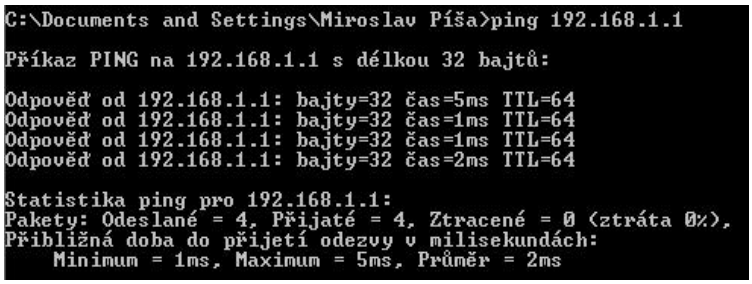


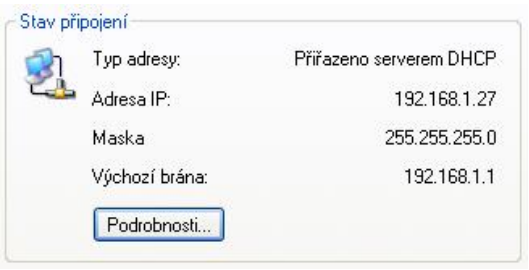
Z toho to zobrazení je patrné v jakém módu zařízení pracuje, informace o připojení k síti a konfigurace LAN rozhranní.

Tímto bylo vše potřebné nastaveno a tak jsem provedl přenastavení síťového rozhraní PC z ruční konfigurace na klienta DHCP serveru.

2 Závěr

Zařízení OvisLink WL-5460 bylo nastaveno do módu klient, kdy se připojilo k nezabezpečené bezdrátové síti wifi_ucebna. Funkčnost připojení byla ověřena získáním IP adresy ze serveru DHCP pro klientský PC a následně i příkazem ping na bránu sítě.





V jakých režimech může zařízení pracovat je vidět na druhém obrázku.
V informacích o sítích v dosahu zařízení je zobrazen název sítě (SSID), MAC adresa vysílacího zařízení (BSSID),vysílací kanál (Channel), tip vysílacího zařízení (Type), použité zabezpečení v síti (Encrypt), síla signálu (Signal).

Univerzita Tomáše Bati ve Zlíně Fakulta aplikované informatiky	
Vypracoval: Bc. Miroslav PÍŠA	Ročník / Skupina:
Předmět: **Zkušební realizace Diplomové práce**	Datum:
Úloha: **2. Přístupový bod OVISLINK 5460, WISP mód (routující klient)**	Hodnocení:

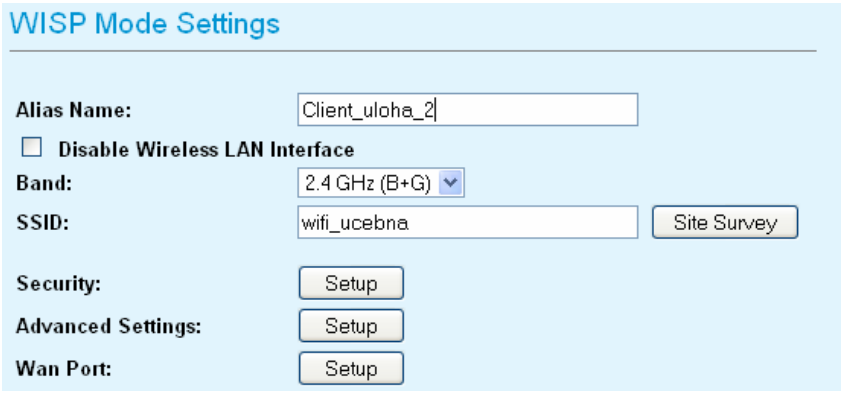
1 Vypracování

Byla provedena ruční konfigurace síťového rozhraní na hodnoty:

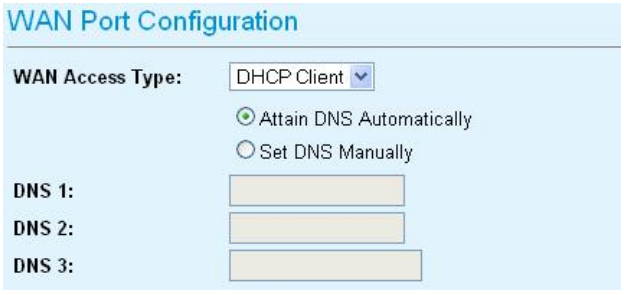
- IP:192.168.0.12/24
- Gate:192.168.0.2

Přes webový prohlížeč jsem se připojily k administračnímu rozhranní zařízení, z operačních módů byl vybrán mód WISP a přes tlačítko Setup bylo přikročeno k další konfiguraci tohoto pracovního režimu.

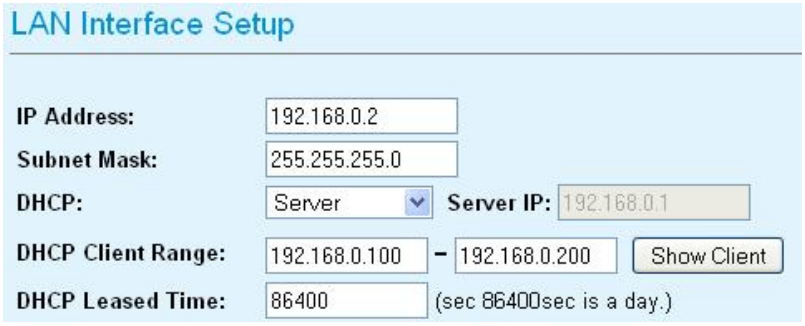
Jako první bylo nastaveno bezdrátové rozhranní, které bude sloužit k připojení zařízení k hostitelské bezdrátové síti *wifi_ucebna*.



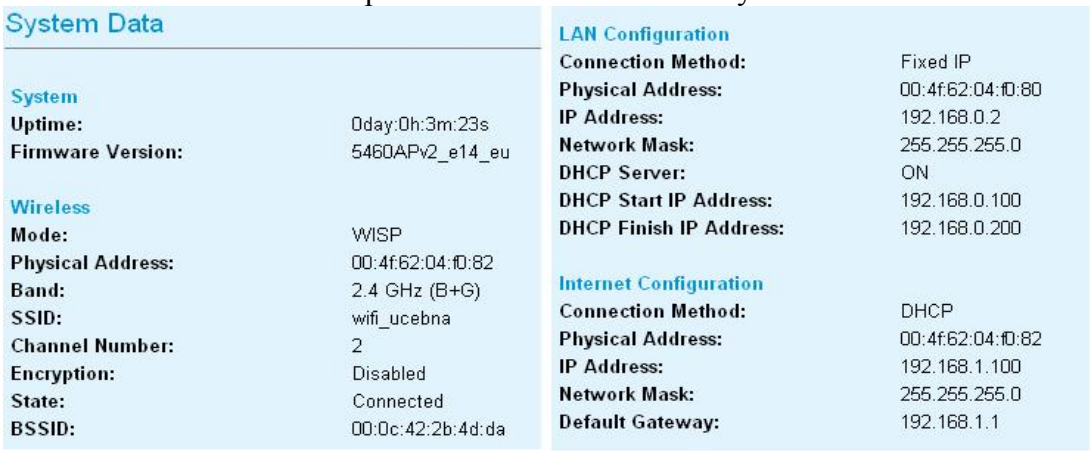
Jelikož nebyla hostitelská síť zabezpečena, pro správnou funkci bylo třeba nastavit ještě WAN rozhranní na IP a DNS z DHCP.



Tím bylo provedeno nastavení klientské části. Dále bylo třeba nastavit LAN rozhranní na lokální síť.



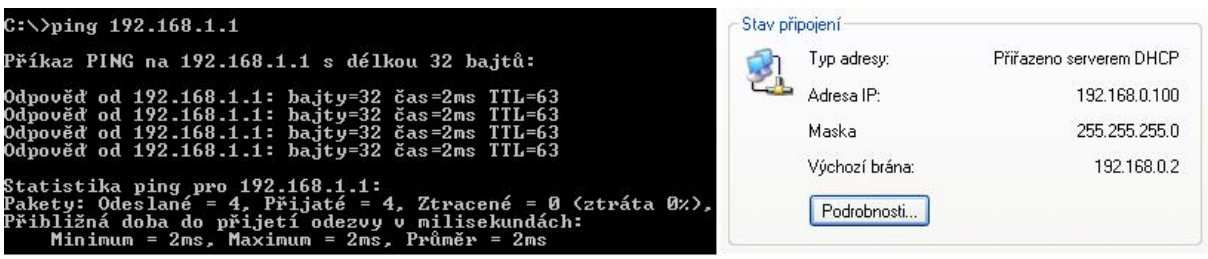
Aby se provedená nastavení uložila a bylo možné otestovat jejich funkčnost, byl proveden restart zařízení a zkontrolována správnost nastavení Status->System



Všechna nastavení souhlasí a proto bylo síťové rozhraní počítače přenastaveno na získání IP z DHCP aby byla ověřena funkčnost celého spojení.

2 Závěr

Zařízení OvisLink WL-5460 bylo nastaveno do režimu WISP, wifi rozhranní bylo připojeno k nezabezpečené bezdrátové síti wifi_ucebna. Rozhranní LAN pak tvořilo samostatnou lokální síť s distribucí IP adres přes DHCP server, který běžel na zařízení OvisLink. Funkčnost připojení byla ověřena získáním IP adresy ze serveru DHCP pro klientský PC. Průchodnost mezi lokální sítí a bezdrátovou sítí, ke které bylo zařízení OvisLink připojeno byla ověřena příkazem ping na bránu bezdrátové sítě.

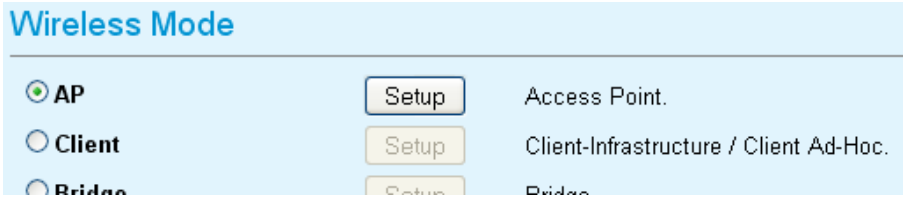


V režimu klient slouží wifi zařízení pouze jako přechod mezi bezdrátovou a metalickou částí sítě. Hostitelský počítač se tak připojuje přímo k zařízení, které distribuuje bezdrátovou síť.
V režimu WISP na LAN běží lokální síť a wifi rozhranní slouží k připojení k hostitelské síti. Tento režim tedy odděluje lokální síť od sítě hostitelské.

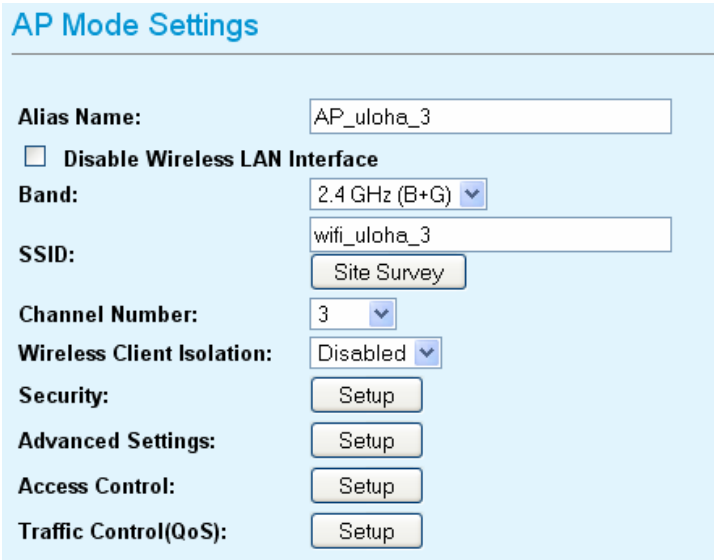
Univerzita Tomáše Bati ve Zlíně Fakulta aplikované informatiky	
Vypracoval: Bc. Miroslav PÍŠA	Ročník / Skupina:
Předmět: **Zkušební realizace Diplomové práce**	Datum:
Úloha: **3. Přístupový bod OVISLINK 5460 jako AP**	Hodnocení:

1 Vypracování

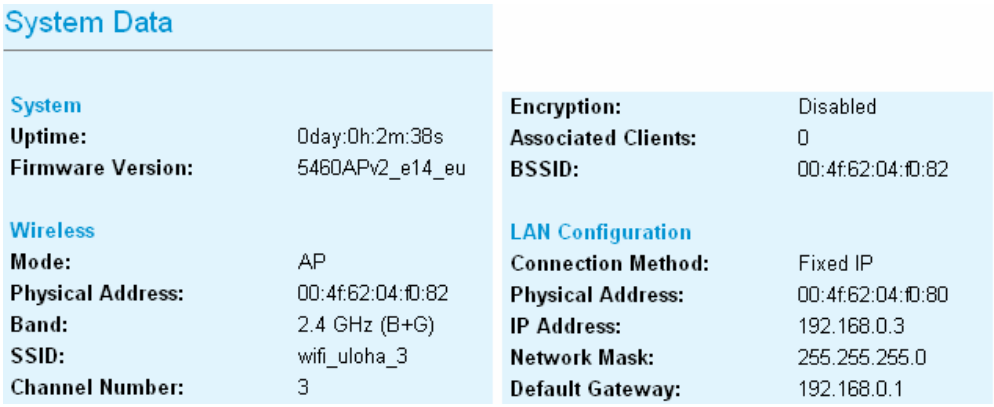
Pomocí webového prohlížeče jsem se připojil ke konfiguračnímu rozhraní zařízení na adrese 192.168.0.2/24. Na úvodní stránce jsem vybral mód AP a kliknutím na tlačítko Setup jsem přešel na další nastavení zařízení.



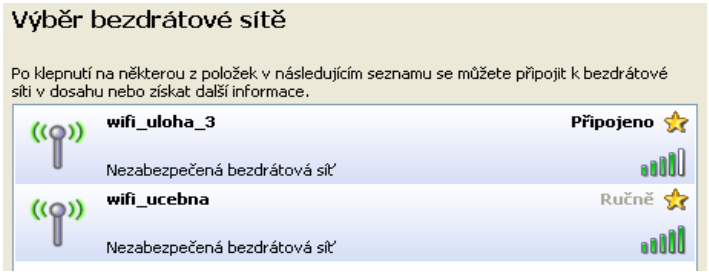
Pro režim AP jsem nastavil Alias Name na AP_uloha_3, pásmo na 2.4 GHz (B+G), SSID na wifi_uloha_3 a vysílací kanál na 3.



Jelikož je toto nastavení dostatečné, tlačítkem Apply Changes jsem nastavení uložil. Aby se uložené nastavení projevilo, bylo třeba zařízení restartovat. Následně jsem provedené nastavení zkontroloval na stránce Status->Systém Data.

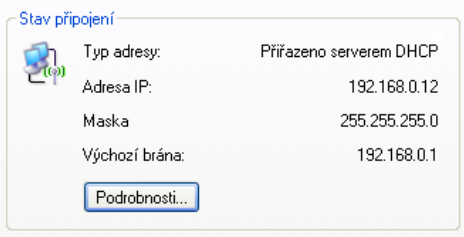


Tímto bylo veškeré potřebné nastavení provedeno a proto jsem PC odpojil od sítě a aktivoval jsem bezdrátovou kartu. Bezdrátové rozhranní bylo nastaveno na IP z DHCP. Z nabízených sítí v dosahu jsem vybral mnou vytvořenou a úspěšně jsem se k ní připojil.



2 Závěr

Zařízení OvisLink WL-5460 bylo nastaveno do módu AP. Funkčnost připojení byla ověřena získáním IP adresy ze serveru DHCP pro klientský PC a následně i příkazem ping na bránu sítě.



Frekvence jednotlivých nabízených kanálu zobrazuje následující tabulka:

Kanál	Frekvence [GHz]	Kanál	Frekvence [GHz]
1	2401-2423	8	2436-2458
2	2406-2428	9	2441-2463
3	2411-2433	10	2446-2468
4	2416-2438	11	2451-2473
5	2421-2443	12	2456-2478
6	2426-2448	13	2461-2483
7	2431-2453	14	2466-2488

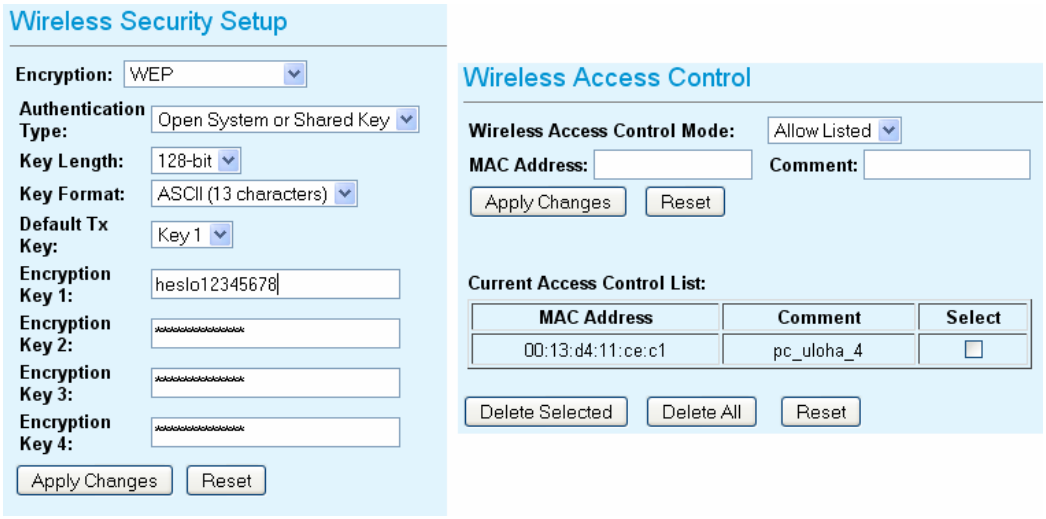
Univerzita Tomáše Bati ve Zlíně Fakulta aplikované informatiky	
Vypracoval: Bc. Miroslav PÍŠA	Ročník / Skupina:
Předmět: **Zkušební realizace Diplomové práce**	Datum:
Úloha: **4. Přístupový bod OVISLINK 5460, základní zabezpečení sítě**	Hodnocení:

1 Vypracování

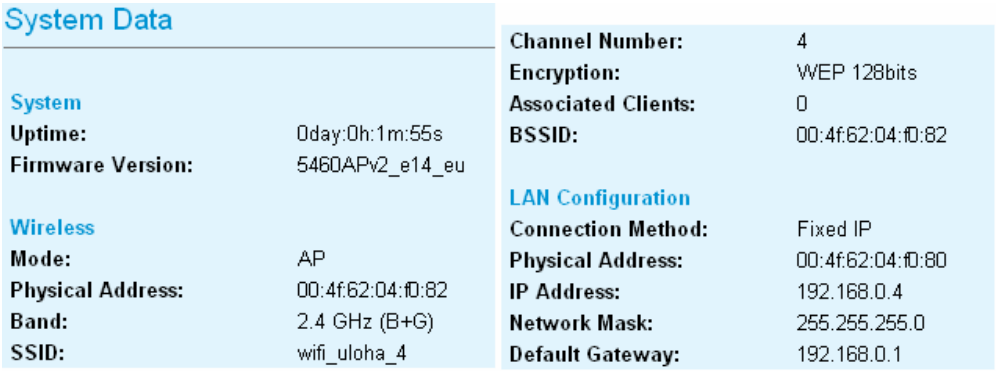
Pomocí webového prohlížeče jsem se připojil ke konfiguračnímu rozhraní zařízení na adrese 192.168.0.4/24. Na úvodní stránce jsem vybral mód AP a kliknutím na tlačítko Setup jsem přešel na další nastavení zařízení.

Nastavil jsem Alias Name na AP_uloha_4, pásmo na 2.4 GHz (B+G), SSID na wifi_uloha_4 a vysílací kanál na 4.

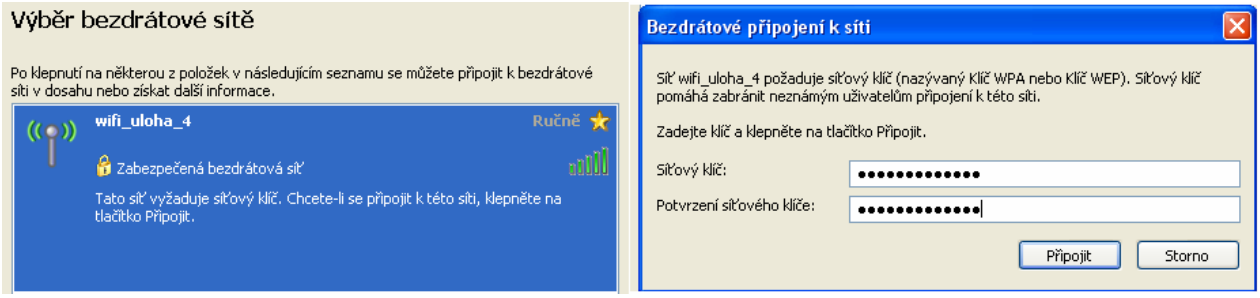
Přes tlačítko Security: Setup jsem přešel na nastavení zabezpečení, zvolil jsem šifrování: WEP, délku klíče: 128b, reprezentaci klíče ASCII a klíč: heslo12345678. Uložil jsem provedené zmněny.
Jako další sem přes tlačítko Access control: Setup přešel na nastavení filtru MAC adres. Vybral jsem metodu Allow listed, při které je třeba zadat MAC adresu zařízení, které má povolen přístup do sítě. Zadal jsem MAC adresu počítače a uložil jsem provedené zmněny.



Aby se provedené změny projevily, bylo třeba zařízení restartovat. Poté jsem ještě provedl kontrolu nastavení přes Status->System

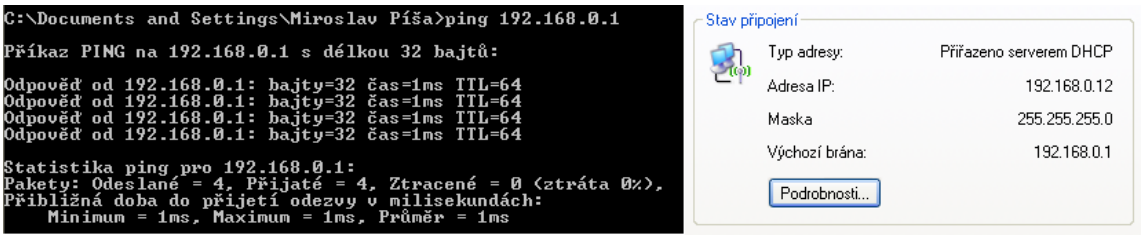


Tímto bylo veškeré potřebné nastavení provedeno a proto jsem PC odpojil od sítě a aktivoval jsem bezdrátovou kartu. Po výběru mnou vytvořené sítě a pokusu o připojení se objevila výzva k zadání hesla. Po jeho zadání se počítač úspěšně připojil k vytvořené síti.



2 Závěr

Zařízení OvisLink WL-5460 bylo nastaveno do módu Access Point. Bezdrátové rozhraní bylo nastaveno na vysílání sítě na 4 kanále pásma 2.4 GHz s SSID wifi_uloha_4. Bezdrátová síť byla zabezpečena šifrováním WEP s délkou klíče 128b a filtrem MAC adres. Po nastavení AP bylo PC odpojeno od metalické sítě a byla aktivována bezdrátová síťová karta. Ze seznamu okolních byla vybrána síť wifi_uloha_4, při pokusu o připojení byl zadán síťový klíč a PC se k ní následně úspěšně připojilo. Toto připojení bylo ověřeno úspěšným přidělením IP adresy z DHCP serveru a také příkazem ping na bránu sítě.



Šifrování WEP používá šifru RC4, což se zároveň i jeho největší slabina. Při šifrování se totiž využívá klíč složený z uživatelského jména a tzv. inicializačního vektoru IV a ten se může po čase začít opakovat a proto je možné po odposlechnutí dostatečně velkého množství paketu síťový klíč odhalit. Na toto je možné na internetu nalézt velké množství programů.

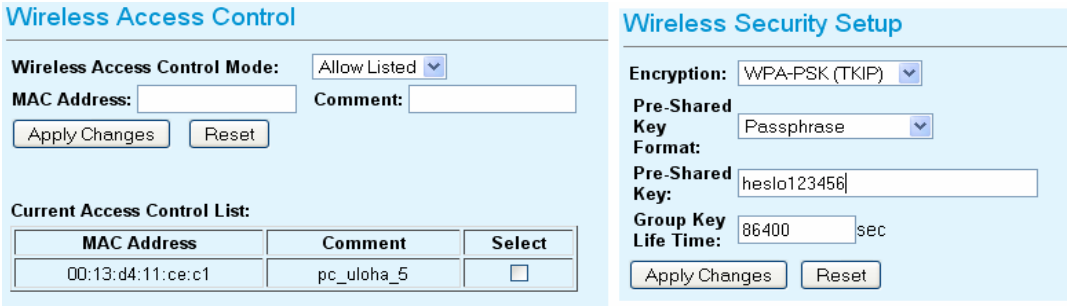
Univerzita Tomáše Bati ve Zlíně Fakulta aplikované informatiky	
Vypracoval: Bc. Miroslav PÍŠA	Ročník / Skupina:
Předmět: **Zkušební realizace Diplomové práce**	Datum:
Úloha: **5. Přístupový bod OVISLINK 5460, pokročilé možnosti zabezpečení pomocí sdíleného klíče**	Hodnocení:

1 Vypracování

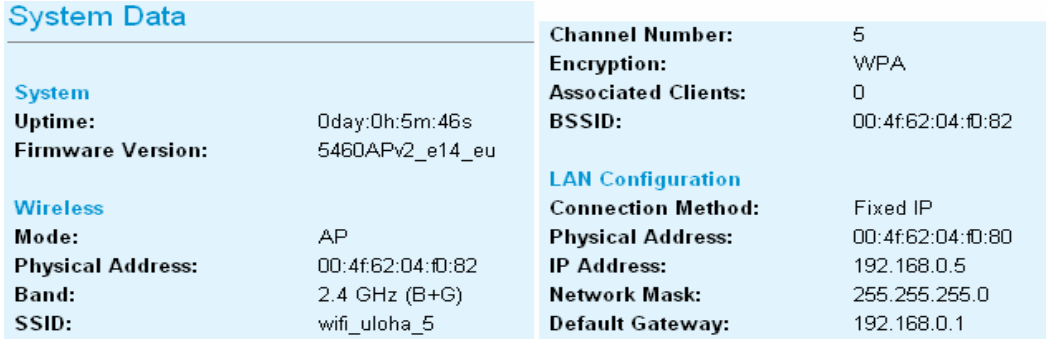
Pomocí webového prohlížeče jsem se připojil ke konfiguračnímu rozhraní zařízení na adrese 192.168.0.5/24. Na úvodní stránce jsem vybral mód AP a kliknutím na tlačítko Setup jsem přešel na další nastavení zařízení.

Nastavil jsem Alias Name na AP_uloha_5, pásmo na 2.4 GHz (B+G), SSID na wifi_uloha_5 a vysílací kanál na 5.

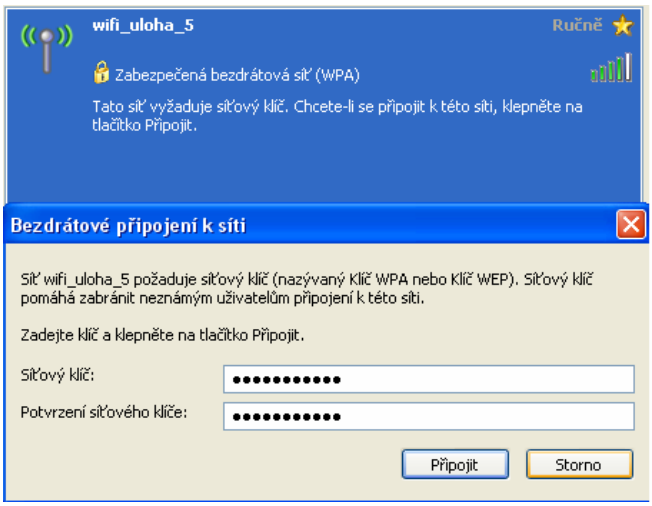
Přes tlačítko Security: Setup jsem přešel na nastavení zabezpečení, zvolil jsem šifrování: WPA-PSK(TKIP), formát klíče: passphrase(heslo), klíč: heslo123456. Uložil jsem provedené zmněny.
Jako další sem přes tlačítko Access control: Setup přešel na nastavení filtru MAC adres. Vybral jsem metodu Allow listed, při které je třeba zadat MAC adresu zařízení, které má povolen přístup do sítě. Zadal jsem MAC adresu počítače a uložil jsem provedené zmněny.



Aby se provedené změny projevily, bylo třeba zařízení restartovat. Poté jsem ještě provedl kontrolu nastavení přes Status->System

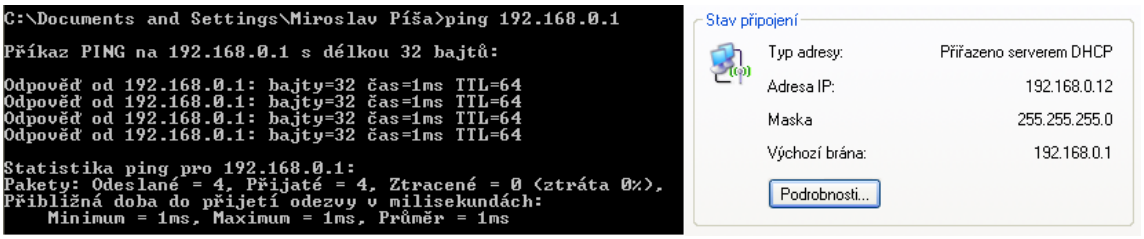


Tímto bylo veškeré potřebné nastavení provedeno a proto jsem PC odpojil od sítě a aktivoval jsem bezdrátovou kartu. Po výběru mnou vytvořené sítě a pokusu o připojení se objevila výzva k zadání hesla. Po jeho zadání se počítač úspěšně připojil k vytvořené síti.



2 Závěr

Zařízení OvisLink WL-5460 bylo nastaveno do módu Access Point. Bezdrátové rozhraní bylo nastaveno na vysílání sítě na 5 kanále pásma 2.4 GHz s SSID wifi_uloha_5. Bezdrátová síť byla zabezpečena šifrováním WPA-PSK(TKIP) a filtrem MAC adres. Po nastavení AP bylo PC odpojeno od metalické sítě a byla aktivována bezdrátová síťová karta. Ze seznamu okolních byla vybrána síť wifi_uloha_5, při pokusu o připojení byl zadán síťový klíč a PC se k ní následně úspěšně připojilo. Toto připojení bylo ověřeno úspěšným přidělením IP adresy z DHCP serveru a také příkazem ping na bránu sítě.



Metoda WPA používá šifrování TKIP, metoda WPA 2 šifrování AES. Tyto metody jsou považovány za dostatečně bezpečné, i když šifrování TKIP využívá šifru RC4, stejně jako WEP a to sebou nese jistou míru rizika. Šifra AES je doposud považována za nerozluštitelnou. Za největší slabinu mnou zvoleného řešení bych považoval použití sdíleného klíče pro přístup do sítě a to z důvodu možnosti jeho vyzrazení.

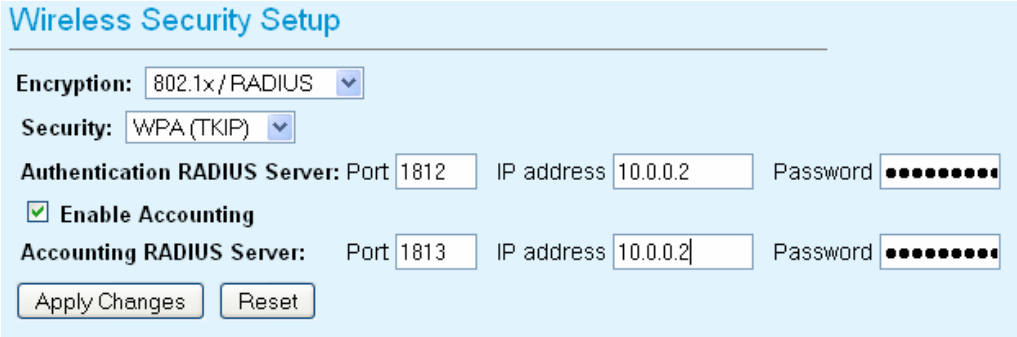
Univerzita Tomáše Bati ve Zlíně Fakulta aplikované informatiky	
Vypracoval: Bc. Miroslav PÍŠA	Ročník / Skupina:
Předmět: **Zkušební realizace Diplomové práce**	Datum:
Úloha: **6. Přístupový bod OVISLINK 5460, pokročilé možnosti zabezpečení pomocí autetizačního serveru RADIUS**	Hodnocení:

1 Vypracování

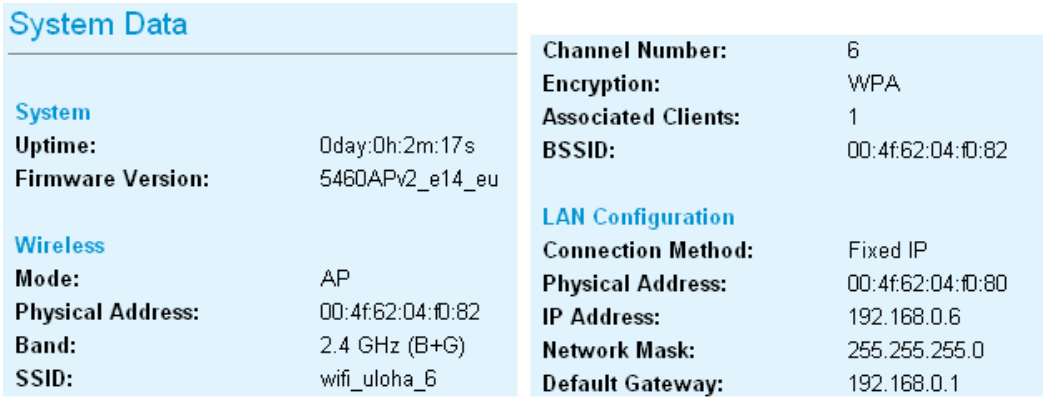
Pomocí webového prohlížeče jsem se připojil ke konfiguračnímu rozhraní zařízení na adrese 192.168.0.6/24. Na úvodní stránce jsem vybral mód AP a kliknutím na tlačítko Setup jsem přešel na další nastavení zařízení.

Nastavil jsem Alias Name na AP_uloha_6, pásmo na 2.4 GHz (B+G), SSID na wifi_uloha_6 a vysílací kanál na 6.

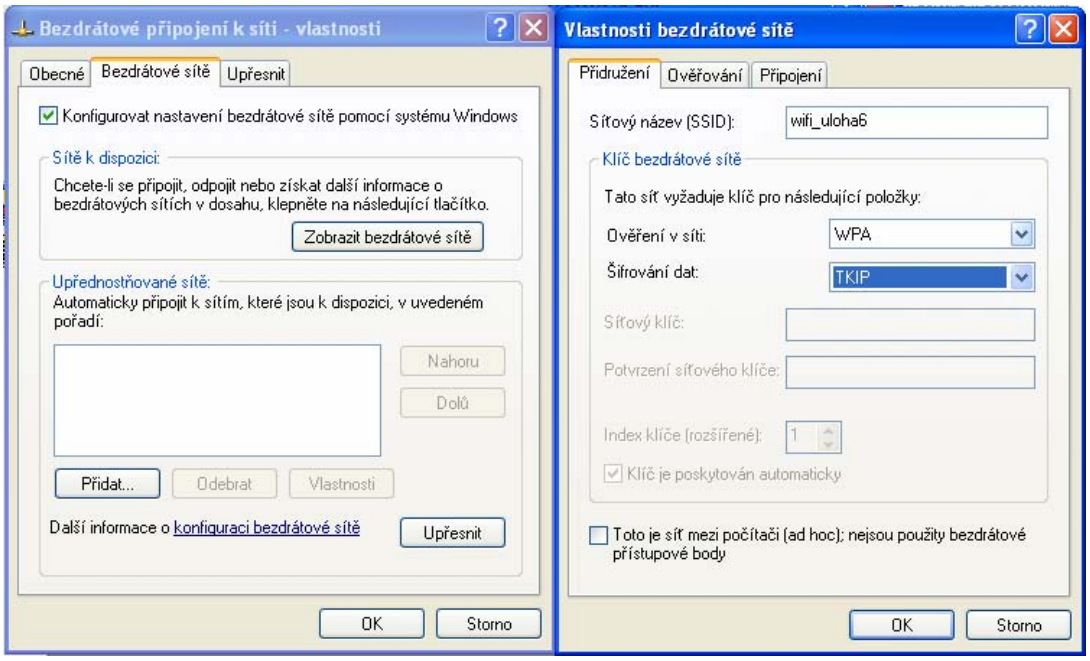
Přes tlačítko Security: Setup jsem přešel na nastavení zabezpečení, zvolil jsem metodu zabezpečení: 802.1x/RADIUS, metoda šifrování: WPA(TKIP), další potřebné údaje jsem vyplnil dle zadání. Uložil jsem provedené změny.



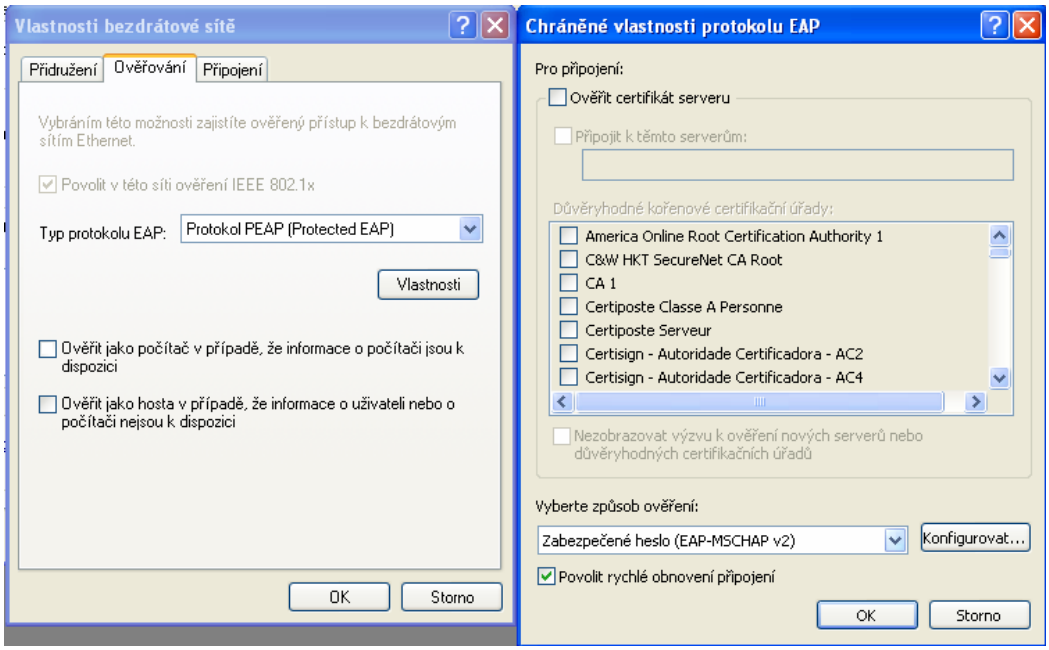
Aby se provedené změny projevily, bylo třeba zařízení restartovat. Poté jsem ještě provedl kontrolu nastavení přes Status->System



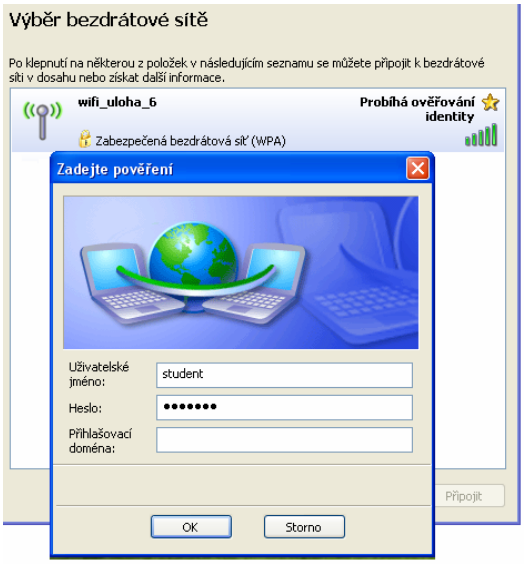
Tímto bylo veškeré potřebné nastavení provedeno a proto jsem PC odpojil od sítě a aktivoval jsem bezdrátovou kartu. Pro připojení k síti bylo třeba nastavit vlastnosti bezdrátového připojení.
V kartě Bezdrátové sítě jsem kliknul na tlačítko Přidat a vyplnil jsem potřebné údaje.



Dále jsem přešel na záložku Ověřování, vybral jsem Typ protokolu EAP: Protokol PEAP a zrušil jsem zaškrtnutí položek Ověřit jako počítač… a Ověřit jako hosta.
Dále jsem kliknul na Vlastnosti a zrušil jsem zaškrtnutí položky Ověřit certifikát serveru, způsob ověření jsem změnil na Zabezpečené heslo (EAP-MSCHAP v2) a zaškrtnul jsem položku Povolit rychlé obnovení připojení. U položky Vyberte způsob ověření jsem kliknul na tlačítko Konfigurovat. Zde jsem zrušil zaškrtnutí položky Automaticky použít přihlašovací jméno, heslo a doménu sys. Windows.

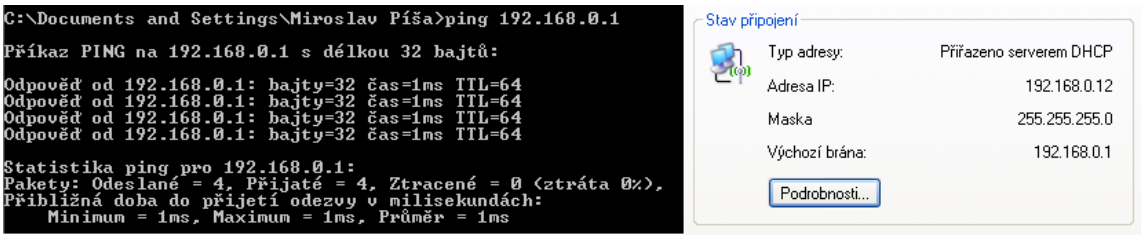


Po nakonfigurování se při pokusu o připojení k sítí objevila výzva k zadání jména a hesla. Zadal jsem hodnoty Jméno: student, heslo: student. Následně se počítač úspěšně připojil k síti a byla mu serverem DHCP přidělena IP adresa.



2 Závěr

Zařízení OvisLink WL-5460 bylo nastaveno do módu Access Point. Bezdrátové rozhraní bylo nastaveno na vysílání sítě na 6 kanále pásma 2.4 GHz s SSID wifi_uloha_6. Bezdrátová síť byla zabezpečena pomoci autentifikace vůči serveru RADIUS a šifrováním WPA-TKIP. Po nastavení AP bylo PC odpojeno od metalické sítě a byla aktivována bezdrátová síťová karta. Bylo provedeno potřebné nakonfigurování připojení pro autentifikaci vůči RADIUS serveru. Při pokusu o připojení bylo zadáno jméno a heslo s hodnotami student/student a PC se k ní následně úspěšně připojilo. Toto připojení bylo ověřeno úspěšným přidělením IP adresy z DHCP serveru a také příkazem ping na bránu sítě.



Klienta lze autentifikovat vedle spojení jméno/heslo i například pomocí bezpečnostních certifikátů.

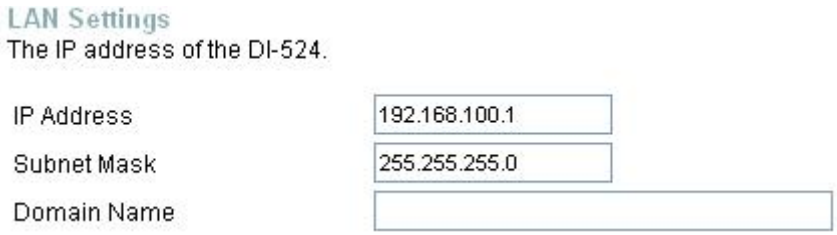
Univerzita Tomáše Bati ve Zlíně Fakulta aplikované informatiky	
Vypracoval: Bc. Miroslav PÍŠA	Ročník / Skupina:
Předmět: **Zkušební realizace Diplomové práce**	Datum:
Úloha: **7. WiFi router D-Link DI-524, nastavení WLAN a LAN, pokročilé zabezpečení WLAN pomocí autentizačního serveru RADIUS**	Hodnocení:

1 Vypracování

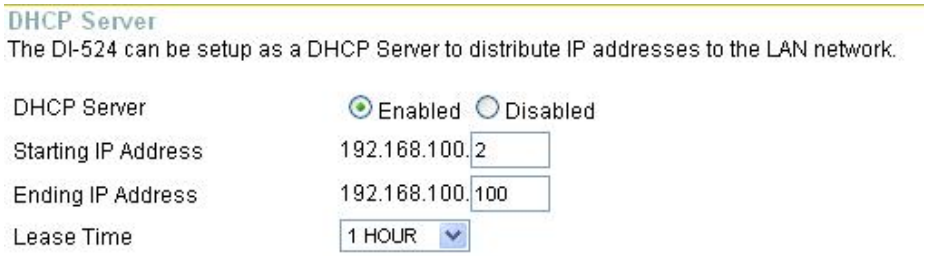
Připojil jsem počítač síťovým kabelem k LAN portu č.1 zařízení D-Link. Po připojení se načetla IP adresa na počítači a ze získaných dat jsem zjistil IP adresu zařízení.
Pomocí webového prohlížeče jsem se připojil ke konfiguračnímu rozhraní zařízení na adrese 192.168.100.1. Před zobrazením administračního rozhranní bylo třeba zadat logovací údaje admin/student.

Jako první jsem kliknul na tlačítko Wireless a provedl jsem nastavení bezdrátového rozhranní. SSID: wifi_uloha_7, kanál: 7, security: WPA, šifrování: TKIP. Dále pak hodnoty pro autentifikaci 802.1x, RADIUS IP: 10.0.0.2, port: 1812, Shared key: testing123.

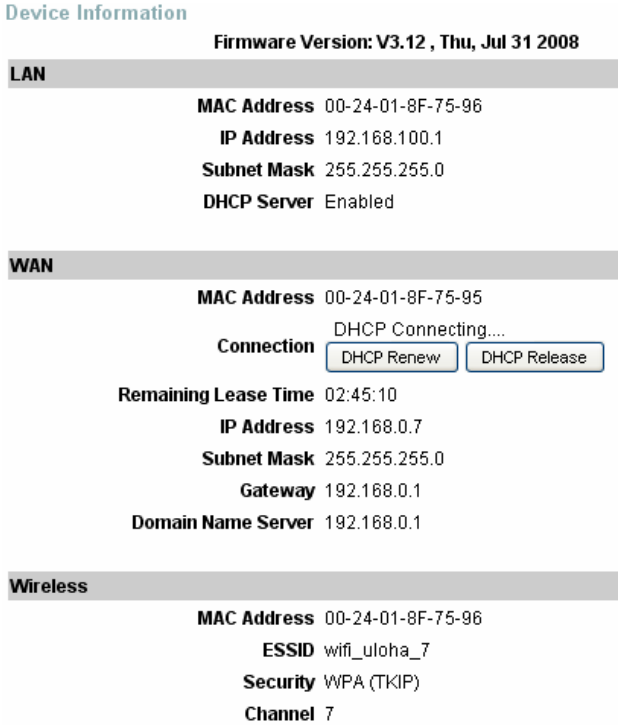
Potom jsem kliknul na tlačítko LAN a provedl nastavení LAN rozhranní.



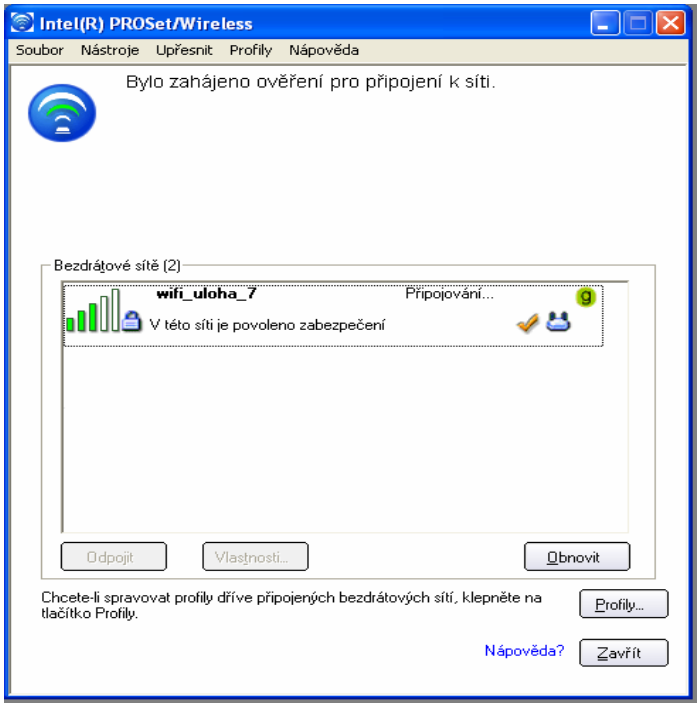
Nakonec jsem nastavil server DHCP pod tlačítkem DHCP:



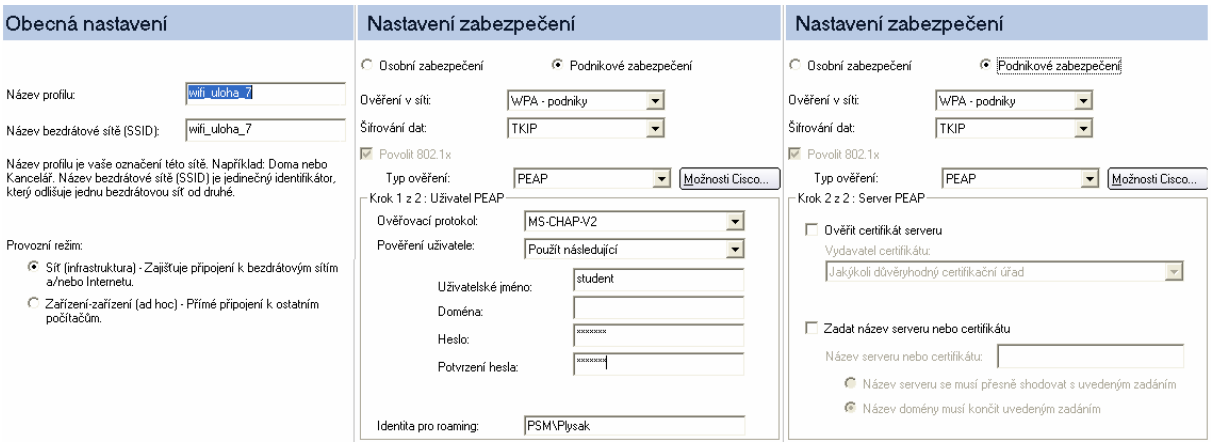
Tím bylo provedeno veškeré potřebné nastavení. Nastavené hodnoty byly ještě zkontrolovány na stránce Device information, záložka Status.



Tímto bylo veškeré potřebné nastavení provedeno a proto jsem PC odpojil od sítě a aktivoval jsem bezdrátovou kartu. Ke zprávě bezdrátového připojení bylo využito programu Intel PROSet/Wireless



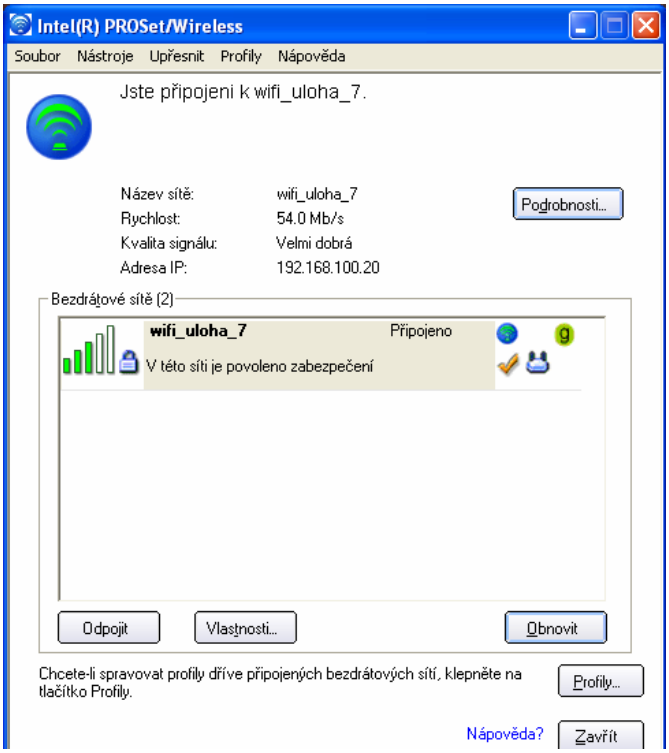
Z nalezených sítí byla vybrána síť wifi_uloha_7 a při pokusu o připojení program sám detekoval použitou metodu zabezpečení a v dalším okně zobrazil potřebné nastavení, stačilo jen doplnit jméno a heslo a v dalším kroku zrušit ověření certifikátem.



Po uložení nastavení se počítač úspěšně připojil k síti a byla mu serverem DHCP přidělena IP adresa.

2 Závěr

Zařízení OvisLink WL-5460 bylo nastaveno do módu Access Point. Bezdrátové rozhraní bylo nastaveno na vysílání sítě na 7 kanále pásma 2.4 GHz s SSID wifi_uloha_7. Bezdrátová síť byla zabezpečena pomoci autentifikace vůči serveru RADIUS a šifrováním WPA-TKIP. Po nastavení AP bylo PC odpojeno od metalické sítě a byla aktivována bezdrátová síťová karta. Připojení k síti bylo provedeno pomocí programu pro zprávu bezdrátových připojení Intel PROSet/Wireless. Tento program byl schopen sám detekovat použité zabezpečení v síti a pro připojení bylo třeba jen vyplnit jméno a heslo a zrušit použití certifikátu při ověření. Po úspěšném připojení byla počítači přidělena IP adresa z DHCP serveru.



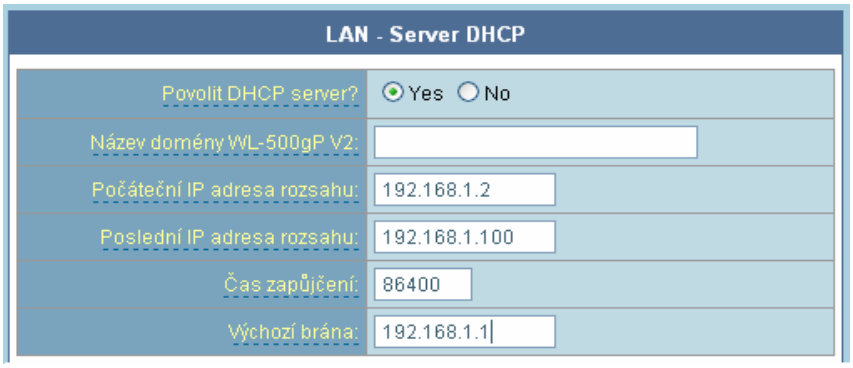
Univerzita Tomáše Bati ve Zlíně Fakulta aplikované informatiky	
Vypracoval: Bc. Miroslav PÍŠA	Ročník / Skupina:
Předmět: **Zkušební realizace Diplomové práce**	Datum:
Úloha: **8. WiFi router ASUS WL-500G, nastavení a zabezpečení sítě, nastavení FTP serveru a stažení dat z připojeného USB disku**	Hodnocení:

1 Vypracování

Připojil jsem počítač síťovým kabelem k LAN portu č.1 zařízení Asus. Po připojení se načetla IP adresa na počítači a ze získaných dat jsem zjistil IP adresu zařízení.
Pomocí webového prohlížeče jsem se připojil ke konfiguračnímu rozhraní zařízení na adrese 192.168.1.1. Před zobrazením administračního rozhranní bylo třeba zadat logovací údaje admin/admin.

Na úvodní stránce grafického administračního rozhranní jsem zadal konfigurační data pro bezdrátovou síť. SSID: wifi_uloha_8, kanál: 8, security: WPA2, šifrování: AES, heslo: heslo123456.

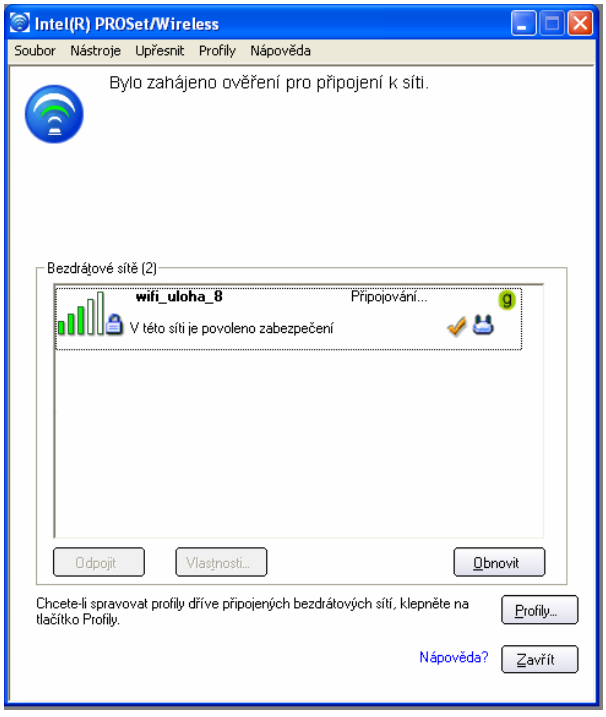
Jako další sem provedl nastavení LAN rozhranní a DHCP serveru



Po nastavení wifi a LAN rozhranní jsem připojil k zařízení externí HDD pomocí USB kabelu. V menu jsem vybral položku USB -> FTP server. V grafickém menu záložky *Sdílený obsah v FTP* se objevil diskový prostor označený part0. Po dalším rozkliknutí této položky se zobrazily jednotlivé složky na disku a přístupová práva k nim. V záložce *Další nastavení* pak bylo možné nastavit další hodnoty jako např. max. počet přihlášených uživatelů, název pracovní skupiny a pod. Omezil jsem poet uživatelů na 1 a všechno ostatní jsem ponechal. Tím byl nastaven FTP disk na adrese 192.168.1.1

Veškerá provedená nastavení jsem ukládal postupně a zařízení po každém uložení provedené změny ihned načetlo. Proto jej nebylo třeba restartovat a mohl jsem přikročit k pokusu o připojení přes bezdrátovou síť.

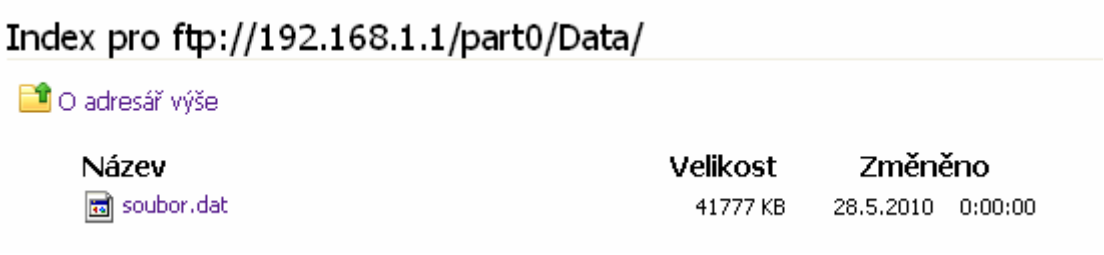
Odpojil jsem PC od sítě a aktivoval jsem bezdrátovou kartu. Ke zprávě bezdrátového připojení bylo využito programu Intel PROSet/Wireless



Z nalezených sítí byla vybrána síť wifi_uloha_8 a při pokusu o připojení program sám detekoval použitou metodu zabezpečení a v dalším okně zobrazil potřebné nastavení pro WPA2-osobní-AES, stačilo jen doplnit síťový klíč *heslo123456* a pokračovat tlačítkem OK.

Po uložení nastavení se počítač úspěšně připojil k síti a byla mu serverem DHCP přidělena IP adresa.

Otevřel jsem webový prohlížeč a zadal jsem adresu ftp://192.168.1.1. Načetl se mi ftp server. Rozkřiknul jsem složku Data a stáhnul jsem soubor *soubor.dat*.



2 Závěr

Zařízení Asus WL-500g Premium bylo nastaveno do módu Access Point. Bezdrátové rozhraní bylo nastaveno na vysílání sítě na 8 kanále pásma 2.4 GHz s SSID wifi_uloha_8. Bezdrátová síť byla zabezpečena pomoci šifrováním WPA2-AES. Dále byl k zařízení připojen externi USB disk a nastaven ftp server na adrese 192.168.1.1. Po nastavení AP bylo PC odpojeno od metalické sítě a byla aktivována bezdrátová síťová karta. Připojení k síti bylo provedeno pomocí programu pro zprávu bezdrátových připojení Intel PROSet/Wireless. Tento program byl schopen sám detekovat použité zabezpečení v síti a pro připojení bylo třeba jen vyplnit síťový klíč. Po úspěšném připojení byla počítači přidělena IP adresa z DHCP serveru. Pomocí webového prohlížeče bylo provedeno připojení na vytvořený ftp server a byl stažen požadovaný soubor.

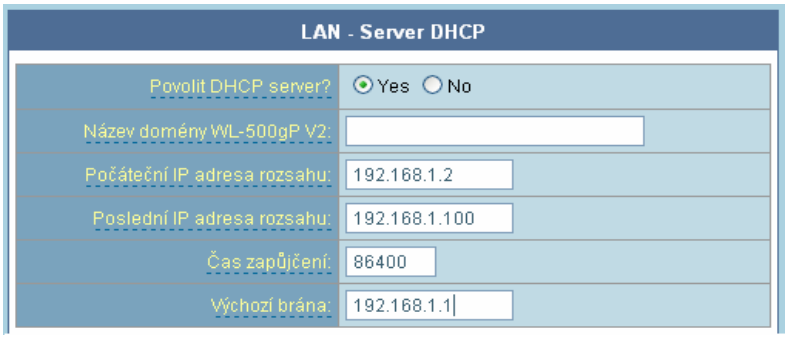
Univerzita Tomáše Bati ve Zlíně Fakulta aplikované informatiky	
Vypracoval: Bc. Miroslav PÍŠA	Ročník / Skupina:
Předmět: **Zkušební realizace Diplomové práce**	Datum:
Úloha: **9. WiFi router ASUS WL-500G, nastavení a zabezpečení sítě, připojení síťové tiskárny**	Hodnocení:

1 Vypracování

Připojil jsem počítač síťovým kabelem k LAN portu č.1 zařízení Asus. Po připojení se načetla IP adresa na počítači a ze získaných dat jsem zjistil IP adresu zařízení.
Pomocí webového prohlížeče jsem se připojil ke konfiguračnímu rozhraní zařízení na adrese 192.168.1.1. Před zobrazením administračního rozhranní bylo třeba zadat logovací údaje admin/admin.

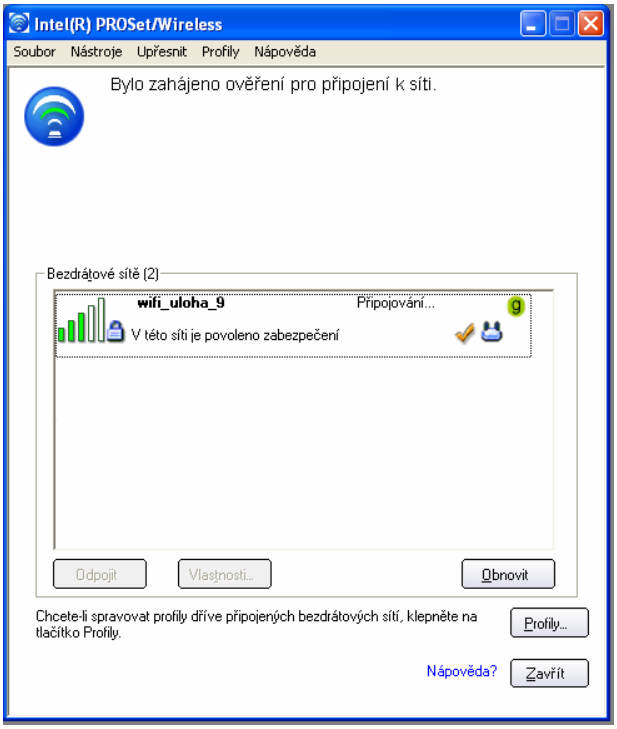
Na úvodní stránce grafického administračního rozhranní jsem zadal konfigurační data pro bezdrátovou síť. SSID: wifi_uloha_9, kanál: 9, security: WPA2-AES, šifrování: AES, heslo: heslo123456.

Jako další sem provedl nastavení LAN rozhranní a DHCP serveru



Po nastavení wifi a LAN rozhranní jsem připojil k zařízení tiskárnu HP PSC 1410. Zařízení samo detekovalo připojené zařízení a automaticky nastavilo IP adresu Print serveru na adresu zařízení 192.168.1.1. Nebylo třeba žádného dalšího nastavení.

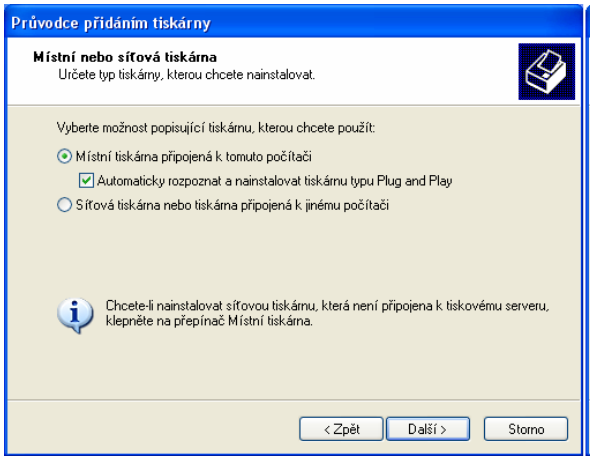
Odpojil jsem PC od sítě a aktivoval jsem bezdrátovou kartu. Ke zprávě bezdrátového připojení bylo využito programu Intel PROSet/Wireless

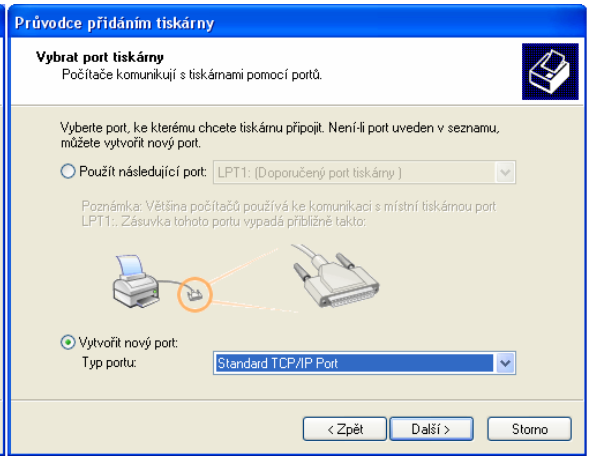


Z nalezených sítí byla vybrána síť wifi_uloha_9 a při pokusu o připojení program sám detekoval použitou metodu zabezpečení a v dalším okně zobrazil potřebné nastavení pro WPA2-osobní-AES, stačilo jen doplnit síťový klíč *heslo123456* a pokračovat tlačítkem OK.

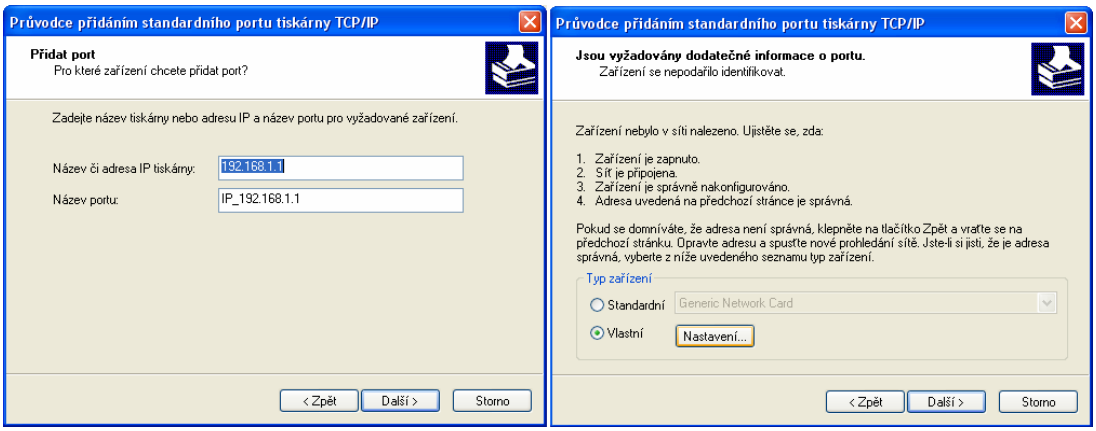
Po uložení nastavení se počítač úspěšně připojil k síti a byla mu serverem DHCP přidělena IP adresa.

Po připojení k síti jsem přistoupil k nastavení síťové tiskárny na počítači. Přes menu Start-> Nastavení-> Tiskárny a faxy-> Přidat tiskárnu jsem spustil průvodce přidáním tiskárny. Vybral jsem Místní tiskárnu a na další stránce jsem vybral Vytvořit nový port: Standard TCP/IP port.

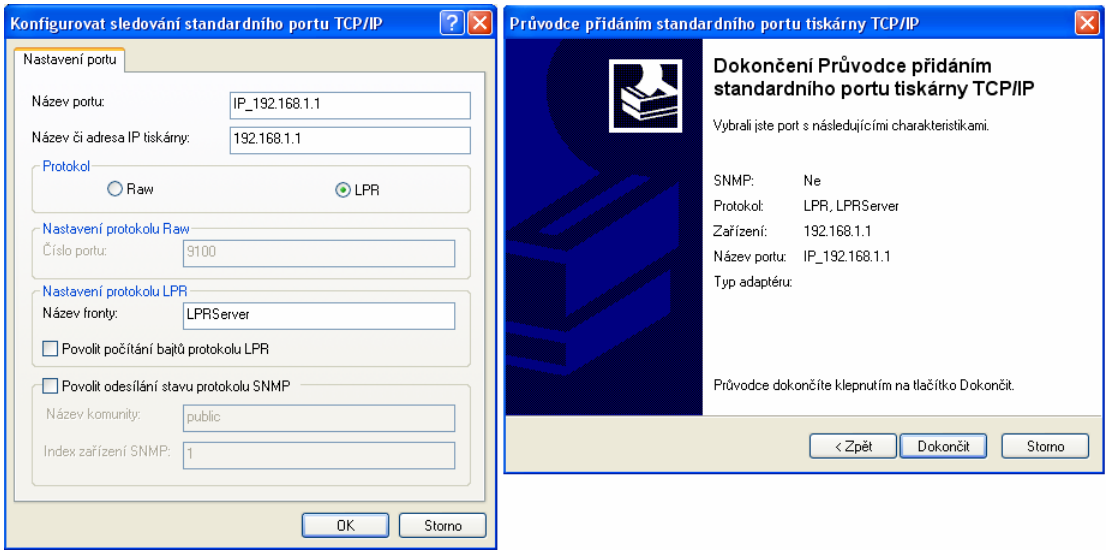




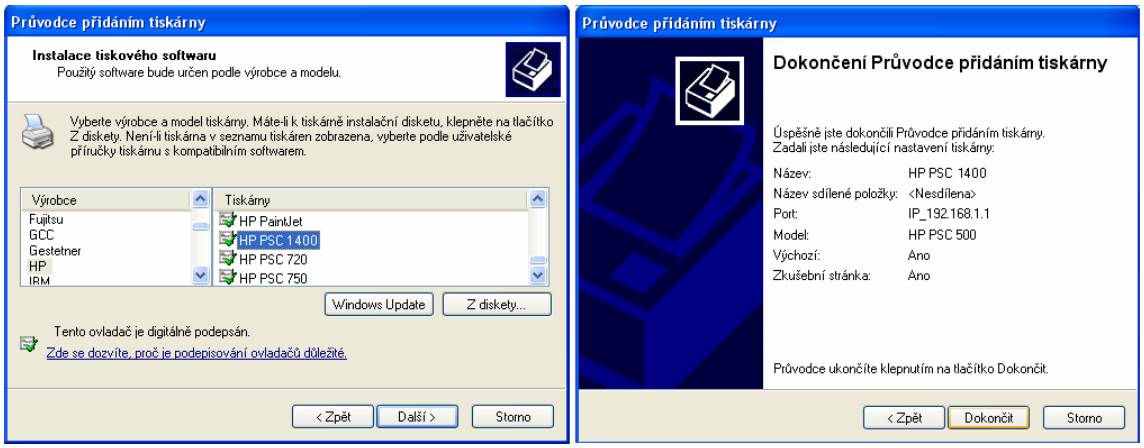
Kliknutím na tl. Další jsem se dostal do menu Nastavení TCP/IP portu. V prvním okně bylo třeba vyplnit IP adresu tiskárny a v dalším okně vybrat volbu Vlastní a přejít na Nastavení.



Vybral jsem protokol LPR a do pole Název fronty sem vyplnil LPRServer. Dále pak OK a Další. Zobrazí se provedené nastavení a dále pak Dokončit.



Následně jsem z nabízených modelů tiskáren vybral vhodný model a tlačítkem dokončit jsem ukončil nastavení. Před dokončením jsem potvrdil vytištění zkušební stránky po dokončení instalace.



2 Závěr

Zařízení Asus WL-500g Premium bylo nastaveno do módu Access Point. Bezdrátové rozhraní bylo nastaveno na vysílání sítě na 8 kanále pásma 2.4 GHz s SSID wifi_uloha_9. Bezdrátová síť byla zabezpečena pomoci šifrováním WPA2-AES. Dále byla k zařízení přes USB port připojena tiskárna a na zařízení se automaticky nastavil print server na adrese 192.168.1.1. Po nastavení AP bylo PC odpojeno od metalické sítě a byla aktivována bezdrátová síťová karta. Připojení k síti bylo provedeno pomocí programu pro zprávu bezdrátových připojení Intel PROSet/Wireless. Tento program byl schopen sám detekovat použité zabezpečení v síti a pro připojení bylo třeba jen vyplnit síťový klíč. Po úspěšném připojení byla počítači přidělena IP adresa z DHCP serveru. Po úspěšném připojení k bezdrátové síti byla provedena instalace síťové tiskárny a po dokončení její instalace proběhlo úspěšné vytištění zkušební stránky.

Univerzita Tomáše Bati ve Zlíně Fakulta aplikované informatiky	
Vypracoval: Bc. Miroslav PÍŠA	Ročník / Skupina:
Předmět: **Zkušební realizace Diplomové práce**	Datum:
Úloha: **10. Zhodnocení vlivu šifrování na šířku přenosového pásma**	Hodnocení:

1 Vypracování

Připojil jsem počítač síťovým kabelem k LAN portu č.1 zařízení Asus. Po připojení se načetla IP adresa na počítači a ze získaných dat jsem zjistil IP adresu zařízení.
Pomocí webového prohlížeče jsem se připojil ke konfiguračnímu rozhraní zařízení na adrese 192.168.1.1. Před zobrazením administračního rozhranní bylo třeba zadat logovací údaje admin/admin.

Na úvodní stránce grafického administračního rozhranní jsem zadal konfigurační data pro bezdrátovou síť. SSID: wifi_uloha_10, kanál: 10.

Jako další sem provedl nastavení LAN rozhranní a DHCP serveru

Stejně jako v úloze 8 jsem připojil USB disk a nastavil ftp server na adrese 192.168.1.1.

Odpojil jsem počítač od metalické sítě, aktivoval jsem bezdrátovou kartu a pomocí programu Intel PROSet/Wireless jsem se připojil k vytvořené síti.

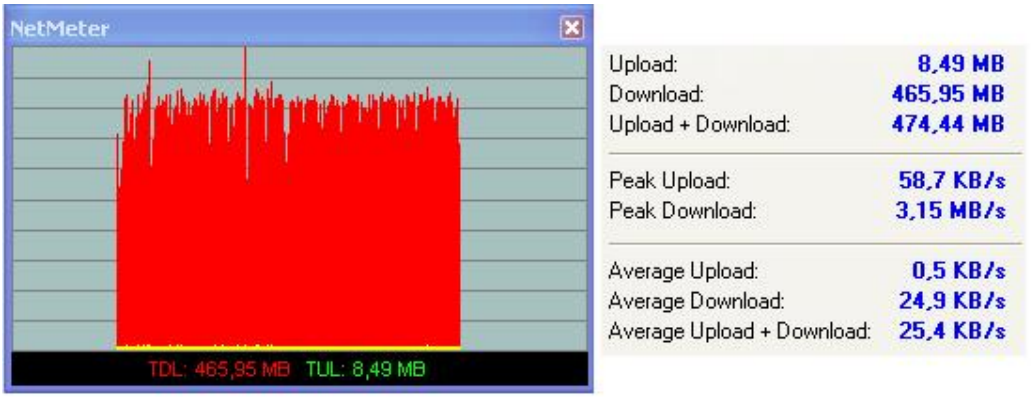
Spustil jsem program NetMeter a přes menu Options jsem upravil vzhled zobrazovaného grafu dle vlastního uvážení.

Vynuloval jsem všechny hodnoty a provedl jsem stažení souboru z disku. Průběh stahovaní byl monitorován programem NetMeter. Po stažení souboru jsem uložil graf rychlosti stahování a připojil jsem i údaje o velikosti přenesených dat.

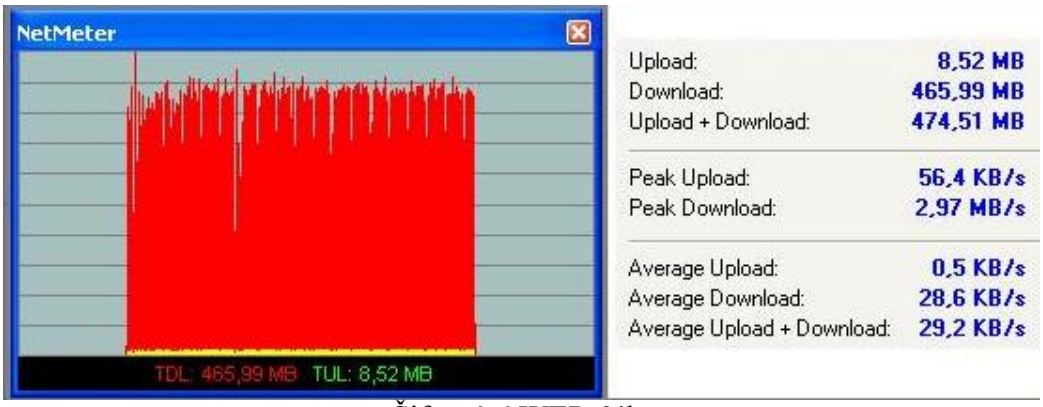
Poté jsem se opět připojil k administračnímu rozhraní zařízení ASUS, změnil jsem zabezpečení sítě nejprve na WEP 64b., WEP 128b., WPA-TKIP a nakonec WPA2-AES. Po každé změně šifrování jsem se znovu připojil pomocí bezdrátové karty k ftp serveru, stáhnul jsem soubor a monitoroval jsem průběh přenosu.

2 Závěr

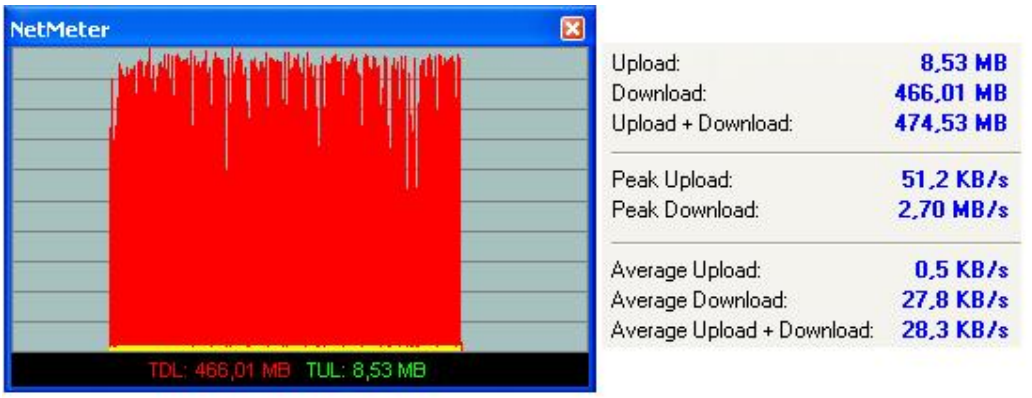
Zařízení Asus WL-500g Premium bylo nastaveno do módu Access Point. Bezdrátové rozhraní bylo nastaveno na vysílání sítě na 10 kanále pásma 2.4 GHz s SSID wifi_uloha_10. Síť nebyla zabezpečena. K zařízení byl připojen USB disk a nastavena funkce ftp serveru. K připojení PC k vytvořené wifi síti byl využit program IntelPROSet/Wireless, přes webový prohlížeč bylo realizováno připojení k ftp serveru a byl stažen soubor soubor.dat. Průběh přenosu byl monitorován pomocí programu NetMeter. Po stažení byla získaná data a graf o přenosu uložena a následně bylo nastaveno zabezpečení wifi sítě nejprve na WEP 64b., poté na WEP 128b., WPA-TKIP a WPA2-AES. Po každé změně zabezpečení bylo provedeno nové připojení k bezdrátové síti a stažení soboru z ftp serveru. Přenos souboru byl vždy monitorován programem NetMeter. Následné grafy zobrazují jednotlivé průběhy:



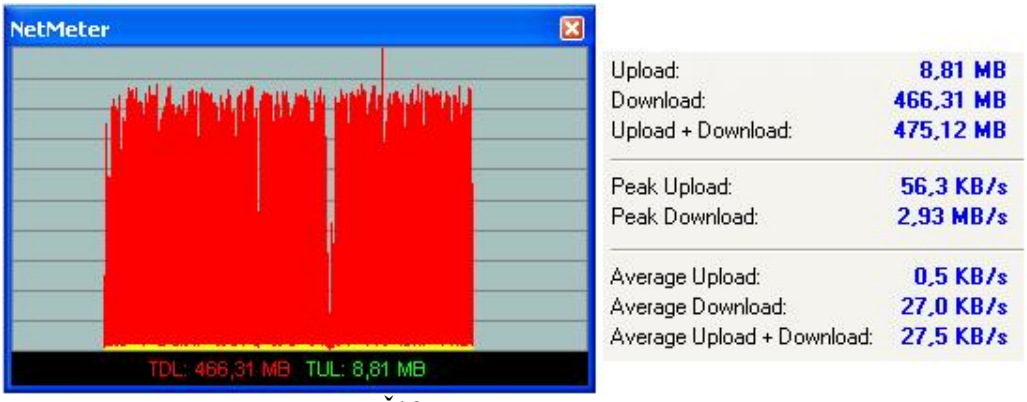
Síť bez zabezpečení



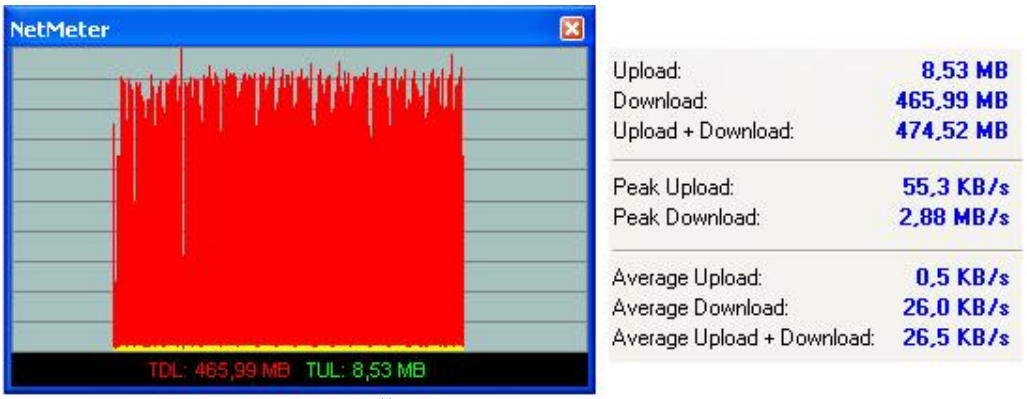
Šifrování WEP 64b.



Šifrování WEP 128b.



Šifrování WPA-TKIP



Šifrování WPA2-AES

Tabulka průměrných hodnot download a upload

	Průměr download [KB/s]	Průměr upload [KB/s]
Otevřený systém	24,9	0,5
WEP 64b.	28,6	0,5
WEP 128b.	27,8	0,5
WPA-TKIP	27,0	0,5
WPA2-AES	26,0	0,5

Z grafů a také z tabulky hodnot průměrné rychlosti stahování je patrné, že zvolená metoda šifrování má minimální vliv na propustnost bezdrátové sítě mezi klientem a přístupovým bodem. Paradoxně nejnižší průměrné hodnoty při stahování soboru dosáhla síť bez zabezpečení.

PŘÍLOHA P II: OBSAH CD

Konfigurační soubory RADIUS serveru:

CD:\Nastavení_RADIUS\radiusd.conf

CD:\Nastavení_RADIUS\eap.conf

CD:\Nastavení_RADIUS\sql.conf

Záloha nastavení routerboardu MikroTik

CD:\Nastavení_Mikrotik\MikroTik.backup

Záloha nastavení jednotlivých zařízení z lab. úloh

CD:\ Záloha_Nastavení_lab_ulohy\config_01.dat

CD:\ Záloha_Nastavení_lab_ulohy\config_02.dat

CD:\ Záloha_Nastavení_lab_ulohy\config_03.dat

CD:\ Záloha_Nastavení_lab_ulohy\config_04.dat

CD:\ Záloha_Nastavení_lab_ulohy\config_05.dat

CD:\ Záloha_Nastavení_lab_ulohy\config_06.dat

CD:\ Záloha_Nastavení_lab_ulohy\config_07.bin

CD:\ Záloha_Nastavení_lab_ulohy\config_08.bin

CD:\ Záloha_Nastavení_lab_ulohy\config_09.bin

CD:\ Záloha_Nastavení_lab_ulohy\config_10.bin

Výstupní soubory tutoriálu k zařízení OvisLink

CD:\ Tutoriál_OvisLink_WL_5460\Exe\OvisLink_WL_5460.exe

CD:\ Tutoriál_OvisLink_WL_5460\Flash\OvisLink_WL_5460.htm

CD:\ Tutoriál_OvisLink_WL_5460\Pdf\OvisLink_WL_5460.pdf