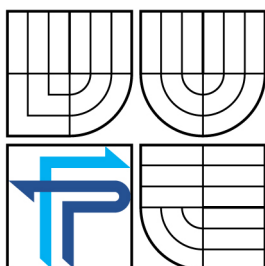


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY
FACULTY OF BUSINESS AND MANAGEMENT
INSTITUT OF INFORMATICS

PROBLEMATIKA BEZDRÁTOVÝCH SÍTÍ

WI-FI NETWORKS ASPECTS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

JIŘÍ SURYNEK

VEDOUCÍ PRÁCE
SUPERVISOR

Doc. Ing. MILOŠ KOCH, CSc.

BRNO 2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jiří Surynek

Manažerská informatika (6209R021)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává bakalářskou práci s názvem:

Problematika bezdrátových sítí

v anglickém jazyce:

Wi-Fi Networks Aspects

Pokyny pro vypracování:

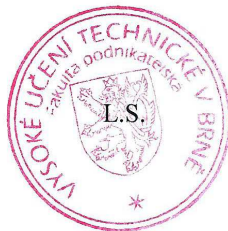
Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza problému
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

- BARKEN, Lee. Wi-Fi: jak zabezpečit bezdrátovou síť. 1.vyd. Brno: Computer Press, 2004. 174 s. ISBN 80-251-0346-3.
- BRISBIN, Shelly. Wi-fi: postavte si svou vlastní wi-fi síť. 1.vyd. Praha: Neocortex, 2003. 248 s. ISBN 80-86330-13-3.
- KÖHRE, Thomas. Stavíme si bezdrátovou síť Wi-fi. 1.vyd. Brno: Computer Press, 2004. 296 s. ISBN 80-251-0391-9.
- ZANDL, Patrick. Bezdrátové sítě WiFi : praktický průvodce. 1.vyd. Brno: Computer Press, 2003. 190 s. ISBN 80-7226-632-2.

Vedoucí bakalářské práce: doc. Ing. Miloš Koch, CSc.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2009/10.




Ing. Jiří Kříž, Ph.D.
Ředitel ústavu


doc. RNDr. Anna Putnová, Ph.D., MBA
Děkanka

V Brně, dne 7. 2. 2010

Čestné prohlášení

Prohlašuji, že jsem bakalářskou práci na téma: „Problematika bezdrátových sítí“ vypracoval samostatně, na základě uvedené literatury a pod vedením svého vedoucího diplomové práce. Současně souhlasím s využitím práce nebo její části v publikacích školy a jejich akademických pracovníků nebo ve výzkumu školy, s odkazem na zdroj informace v souladu se zákonem č. 121/2000 Sb.

V Brně dne

.....

Jiří Surynek

Bibliografický záznam

SURYNEK, J. *Problematika bezdrátových sítí*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2010. 83 s. ved. bakalářské práce Doc. Ing. Miloš Koch, CSc.

Anotace

Tato práce se zabývá problematikou bezdrátových sítí. Shrnuje technologie použité při bezdrátovém připojení. Zabývá se historií bezdrátového připojení, ale i nástinem budoucích trendů.

Anotation

This work deals with wireless networks. This work summarizes the techniques used in wireless connection. It deals with the history of wireless connectivity, as well as foreshadowing future trends.

Klíčová slova

Bezdrátové síť, bezdrátové připojení, Wi-Fi, WiMAX, IEEE 802.11a/b/g/n, IEEE 802.16e.

Key words

Wireless networks, wireless connection, Wi-Fi, WiMAX, IEEE 802.11a/b/g/n, IEEE 802.16e.

Poděkování

Rád bych na tomto místě poděkoval doc. Ing. Miloši Kochochovi, CSc. za podporu a cenné rady, které mi pomohly při zpracování mé bakalářské práce.

Cíle práce

Informovat o základním termínech používaných při Wi-Fi problematikách, rozvést otázku zabezpečení sítě, návrhy řešení komplikací, přejít k tvorbě vlastní sítě, jejího využití a prakticky ukázat problémy, na které běžně narážíme. Práce by měla objasnit základní pojmy v problematice Wi-Fi sítí, seznámit s technologiemi používanými v souvislosti s Wi-Fi. Ukázat historický vývoj technologií a nastínit jak by se mohly tyto technologie dále vyvíjet.

Obsah

Úvod.....	11
1 Teoretická východiska práce	12
1.1 Historie bezdrátové komunikace	12
1.2 Wi-Fi.....	14
1.2.1 Standard IEEE 802.11.....	14
1.2.2 Standard IEEE 802.11b.....	16
1.2.3 Standard IEEE 802.11a.....	17
1.2.4 Standard IEEE 802.11g.....	18
1.2.5 Standard 802.11n	20
1.2.6 Přehled dodatků ke standardu 802.11	22
1.3 Zabezpečení bezdrátových sítí.....	24
1.3.1 Filtrování MAC adres	24
1.3.2 Skrytí SSID sítě	26
1.3.3 WEP	27
1.3.4 WPA.....	30
1.3.5 WPA2.....	38
1.4 Budoucnost bezdrátových technologií.....	42
2 Analýza problémů.....	44
2.1 Hardware použitý v nynější síti	44
2.2 Zabezpečení nynější bezdrátové sítě.....	53

2.3	Analýza problémů.....	56
3	Vlastní návrhy řešení	57
3.1	FTP server.....	57
3.2	Připojení TV v obývacím pokoji do sítě.....	59
3.3	Zvýšení přenosové rychlosti sítě pro přehrávání 1080p filmů	62
3.4	Umístění serveru	64
3.5	Připojení do sítě pomocí smartphone.....	68
3.6	Shrnutí všech úprav a rozšíření sítě	69
3.7	Ekonomické zhodnocení.....	72
3.7.1	Očekávané finanční náklady	72
3.7.2	Očekávané nefinanční nákladů	73
3.7.3	Očekávané nefinanční přínosy.....	73
	Závěr	74
	Seznam použitých obrázků	75
	Seznam tabulek.....	77
	Seznam použitých zkratk	78
	Seznam použité literatury	81

Úvod

Bezdrátové sítě jsou v dnešní době široce skloňovaným pojmem. Za poslední tři roky se staly fenoménem a jsou využívány prakticky každou domácností s notebookem, smartphonem, nebo více počítači. Technologie, která byla ještě před pár lety doménou velkých firem a v osobní sféře se prakticky nevyskytovala, je dnes prakticky samozřejmostí.

Pod pojmem bezdrátové sítě se neskrývá jen technologie Wi-Fi sítí standardů a/b/g/n, ale i mnoho dalších technologií, některé notoricky známé (Bluetooth, CDMA, EDGE atd.), jiné zná jen několik IT specialistů a počítačových nadšenců (WiMAX, HSDPA atd.). Já se ale budu zabývat jen technologií Wi-Fi. Na začátku této práce se věnuji historii bezdrátového připojení, dále popisuji jednotlivé technologie. Následuje popis technologií používaných k zabezpečení bezdrátových sítí a po té informuji o některých budoucích trendech v oblasti bezdrátových sítích a nastiňuji možnosti dalšího vývoje. Nakonec prezentuji praktickou část mé bakalářské práce a to popis mé vlastní bezdrátové sítě, postavené na Wi-Fi technologii a snažím se ukázat další možnosti jejího rozšíření a vylepšení.

Co se týče přínosů této práce, tak by měla pomoci jak při výstavbě nové sítě, tak při řešení problémů ve stávající síti a pomoci při jejím rozšiřování a modernizaci. Navíc by také měla seznámit laického čtenáře s problematikou jednotlivých technologií a informovat jej o možnostech těchto jednotlivých technologií.

1 Teoretická východiska práce

1.1 Historie bezdrátové komunikace

Prvním člověkem, který úspěšně přenesl nějakou informaci bez pomoci drátů pomocí rádia byl italský vědec Guglielmo Marconi. Tento přenos se uskutečnil v roce 1895 na vzdálenost přibližně dvou kilometrů, pomocí tzv. bezdrátového telegrafu. V roce 1896 si tento přístroj patentoval. O rok později se mu podařil přenos na vzdálenost 15 kilometrů, a 12. prosince 1901 provedl první transatlantické bezdrátové spojení. V roce 1906 byl poprvé rádiově přenesen hlas. Další rozvoj bezdrátových komunikací souvisel především s námořnictvem, protože pozemní komunikace ovládal telegraf, ale také s armádou celkově. „V desátých a dvacátých letech minulého století došlo k velkému a zpočátku naprosto nekontrolovanému rozvoji radiového vysílání. Počátkem dvacátých let se v USA začaly používat mobilní radiové stanice, které fungovaly v pásmu 2 MHz. Používaly je pouze policejní a vojenské složky a většinou šlo pouze o přijímače. Průkopníkem v používání rádia byla detroitská policie, kde v roce 1921 zprovoznili první auto s radiopřijímačem morseovky a o sedm let později již přenášeli také hlas.“¹ V roce 1924 bylo v Bell Laboratories v USA sestrojeno první mobilní rádio, které přenášelo hlas v obou směrech. „V roce 1934 byla demonstrována frekvenční modulace (FM), která ve srovnání s amplitudovou modulací (AM) umožnila kvalitnější přenos zvuku. Ve třicátých letech 20. století začal rozvoj analogové radiotelefonie.“² Velice důležitou roli sehrála bezdrátová komunikace za druhé světové války, kdy se používala přenosná radiovysílačka vyrobená společností Motorola, která byla důležitým prostředkem komunikace na bojišti.

V padesátých letech se objevily první návrhy mobilních rádiových systémů, založených na podobné technologii jako je tomu u dnešních sítí GSM. První mobilní

¹ RAMBOUSEK, Adam. *Fakulta informatiky Masarykovy univerzity* [online]. 2003 [cit. 2010-05-08]. Historie mobilní komunikace. Dostupné z WWW: <http://www.fi.muni.cz/usr/jkucera/pv109/2003/xrambous_index.htm>.

² BRADÁČ, Z., FIEDLER, P., KAČMÁŘ, M. Bezdrátové komunikace v automatizační praxi I: historie a současnost. *Automa* [online]. 2009 [cit. 2009-12-03]. Dostupný z WWW: <http://www.odbornecasopisy.cz/index.php?id_document=28818>.

analogový telefonní přenos byl proveden v roce 1961. Dalším důležitým mezníkem v bezdrátové komunikaci je příchod prvních digitálních telefonních systémů, na konci osmdesátých let 20. století. Nejúspěšnější z nich byly jsou v Evropě systémy GSM. Na konci minulého století pak v prakticky všech oblastech bezdrátové komunikace vévodí digitální řešení. V roce 1997 byl přijat standard IEEE 802.11, který popisuje bezdrátovou komunikaci mezi počítači.

1.2 Wi-Fi

WI-FI je snad nejznámější formou bezdrátové komunikace. Zkratka Wi-Fi znamená Wireless Fidelity (bezdrátová spolehlivost) a Institut inženýrů elektrotechniky (Institute of Electrical and Electronics Engineers – „IEEE vyvíjí a schvaluje normy pro širokou řadu počítačových technologií. Tato organizace vytváří pracovní skupiny technologických expertů, zastupujících dodavatele a vědecké / inženýrské kruhy za účelem studia, přezkoumávání a schválení navrhovaných norem, na kterých pak mohou být založeny nové výrobky.“³), pro ni má pro tuto technologii označení IEEE 802.11 (802 je označení síťové normy, 11 je označení podskupiny bezdrátových sítí).



Obr. 1: Logo standardu Wi-Fi.

1.2.1 Standard IEEE 802.11

Norma IEEE 802.11 jako taková byla přijata v roce 1997. Tato norma pracovala na frekvenci 2,4 GHz, a maximální propustnost byla 2 Mbit/s. Poté přišla úprava normy s názvem IEEE 802.11 High rate, která umožňovala zvýšení rychlosti na 11 Mbit/s. K přejmenování IEEE 802.11 High rate na IEEE 802.11b došlo v roce 1999. Další změnou, která se udála v roce 1999 bylo vytvoření normy IEEE 802.11a, která pracuje na frekvenci 5 GHz a umožňuje vyšší rychlost. Standard IEEE 802.11g byl schválen v roce 2002 a pracuje na frekvenčním pásmu 2,4 GHz a podporuje stejnou rychlost jako

³ BRISBIN, S. *Wi-Fi: postavte si svou vlastní wi-fi síť*. Praha: Neocortex, 2003. 248 s. ISBN 80-291-8644-2.

IEEE 802.11a tedy 54 Mbit/s. V roce 2003 se začalo pracovat na standardu IEEE 802.11n, který byl po dlouhém schvalovacím procesu v roce 2008 schválen. Standard zvyšuje propustnost sítě a to až na teoretických 300 Mbit/s, čímž překonává i dodnes používaný standard IEEE 802.3y – tedy 100 Mbit/s ethernet.

Standard	Rok zavedení	Popis
IEEE 802.11	1997	První standard WLAN s přenosovou rychlostí 1 až 2 Mbps
IEEE 802.11a	1999	WLAN 54Mbps v pásmu 5 GHz
IEEE 802.11b	1999	WLAN 11Mbps v pásmu 2,4 GHz
IEEE 802.11b+	2001	WLAN 22Mbps v pásmu 2,4 GHz
IEEE 802.11g	2001	Wireless LAN 54Mbps v pásmu 2,4 GHz
IEEE 802.1x	2001	Síťový autentizační mechanismus založený na portech, žádný standard Wireless LAN
IEEE 802.11i	2002	Rozšíření 802.11 s novými bezpečnostními prvky
IEEE "802.11e" 108 Mbps	2003	Nestandardizovaný mechanismus zvýšení přenosové rychlosti pomocí Channel Bounding, hardwarové komprese, Packet Bursting a Fast Frames

Obr. 2.: Přehled některých standardů IEEE 802.11.⁴

Standard IEEE 802.11 však nemá jen dodatky a/b/g/n, ale má i další a tyto se už nezaměřují na změny propustnosti sítě nebo nemění frekvenční rozsah. Jedná se spíše o malé úpravy standardu. „IEEE 802.11i je zaměřena na vylepšení zabezpečení bezdrátových sítí, zatímco IEEE 802.11e, je orientována na otázky kvality služeb (QoS), které jsou důležité u velkých bezdrátových sítí. Jakmile jsou tyto normy přijaty, mohou být buď zkonsolidovány do jednoho ze síťových protokolů nebo mohou být jednoduše dány k dispozici dodavatelům, kteří budou chtít přidat nějaké funkční charakteristiky ke svým výrobkům, podle norem 802.1a/b/g nebo n.“⁵

⁴ KÖHRE, T. *Stavíme si bezdrátovou síť Wi-Fi*. Vyd. 1. Brno: Computer Press, 2004. 297 s. ISBN 80-251-0391-9

⁵ BRISBIN, S. *Wi-Fi: postavte si svou vlastní wi-fi síť*. Praha: Neocortex, 2003. 248 s. ISBN 80-291-8644-2.



Obr. 3.: Návrh loga pro zařízení podporující všechny čtyři standardy.

1.2.2 Standard IEEE 802.11b

Tento standard je prvním zásadním dodatkem k normě IEEE 802.11. Jak je uvedeno výše, původně měl přídomek High rate, protože zvyšoval propustnost sítě na 11 Mbit/s. V dnešní době je tento standard již zastaralý a nedostačující. Ve své době však byl důležitým dodatkem, který prakticky normu IEEE 802.11 rozšířil. Většina zařízení byla totiž založena až na standardu 802.11b. Standard 802.11b, používá na rozdíl od standardu 802.11a, jako mechanismus přenosu DSSS (Direct Sequence Spread Spektrum – technika přímého rozprostřeného spektra), což je vlastně umělé zavedení redundance signálu, který je pak rozprostřen do větší části frekvenčního spektra a tudíž je odolnější proti rušení a tak se zvyšuje spolehlivost přenosu. Tento typ modulační techniky bývá využíván nejen ve Wi-Fi komunikaci, ale také třeba v navigačním systému GPS.



Obr. 4.: Apple Air-Port logo.

Jedním z prvních výrobků založených na tomto standardu byl v roce 1999 Air-Port firmy Apple. Součástí Air-Portu byl přístupový bod a PC karta pro notebooky

Macintosh. Firma Apple velmi napomohla rozšíření standardu IEEE 802.11b a díky ní se Wi-Fi dostalo do povědomí veřejnosti a velmi se zpopularizovalo.



Obr. 5.: Apple Air-Port přístupový bod.

1.2.3 Standard IEEE 802.11a

Tento standard byl schválen nedlouho poté, co byl schválen standard IEEE 802.11b. Frekvenční rozsah je 5 GHz. Tento standard stejně jako IEEE 802.11g poskytuje maximální teoretickou rychlost 54 Mbit/s a to díky technologii OFDM (Orthogonal Frequency Division Multiplexing – ortogonální multiplex s kmitočtovým dělením). Signál je u této technologie vysílán na více na sobě nezávislých frekvencích - kanálech, což zvyšuje odolnost proti rušení. OFDM nevyužívá jen při přenosu dat pomocí IEEE 802.11 a/g/n, ale taky pro přenos digitálního televizního signálu DVB-T, dále technologie ADSL nebo WiMAX.

Tento standard byl a je mnohem méně využíván, než standard 802.11b. Důvodem asi bude to, že „zatímco výrobky vyrobené na základě normy 802.11b se objevily krátce poté, co norma získala schválení od IEEE, začala se zařízení vyrobená na základě

normy 802.11a objevovat až v roce 2002⁶. Naopak velkou výhodou je frekvenční pásmo, ve kterém tento standard pracuje – 5 GHz je otevřený a velmi široký rozsah, ve kterém je mnohem méně rušení od ostatní přístrojů a aplikací.

Tato norma měla konkurenční nevýhodu, z hlediska pozdějšího nasazení většiny podporovaného hardwaru. To byl jeden z důvodů, proč při dnešním srovnání byla v době úsvitu bezdrátové Wi-Fi komunikace mnohem úspěšnější norma 802.11b i přes své horší specifikace (nižší maximální přenosová rychlost). I tato technologie stejně jako 802.11b už je na ústupu. Ve většině nových zařízení je sice podporována, ale je to jen z důvodu zpětné kompatibility se starším hardwarem. Velmi zajímavou skutečností je také to, že v době vydání tohoto standardu, nebyl kompatibilní se standardem 802.11b – důsledkem toho bylo, že při vytváření vlastní bezdrátové sítě, jste se museli rozhodnout mezi levnější, ale pomalejší variantou 802.11b nebo rychlejší, ale dražší 802.11a, což je jeden z dalších důvodů nižší obliby standardu 802.11a. V dnešní době je většina zařízení, využívající bezdrátovou komunikaci vybavená podporou jak standardu 802.11a, tak 802.11b (popřípadě 802.11g a 802.11n).

1.2.4 Standard IEEE 802.11g

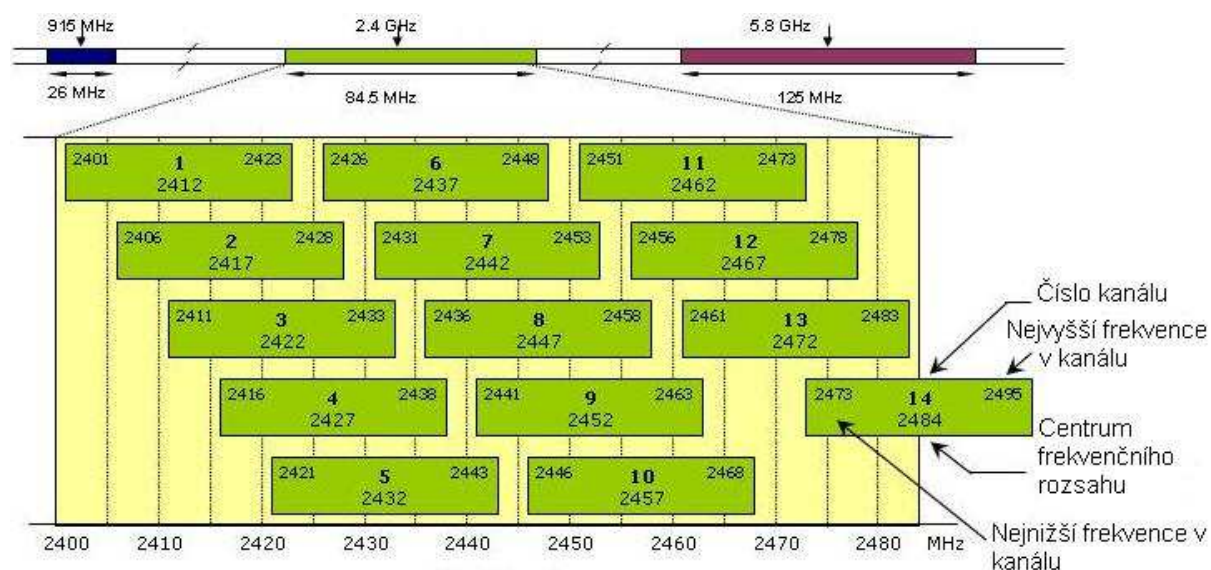
Tento standard je v současné době asi nejpoužívanější. Někdy bývá tato norma také pojmenována IEEE 802.11g-2003. Standard 802.11g byl schválen IEEE v roce 2003. Nabízí již podstatně lepší maximální teoretickou přenosovou rychlost 54 Mbit/s. Stejně jako standard 802.11b pracuje na kmitočtu 2.4 GHz. Také využívá technologii „OFDM jako norma 802.11a s možností, která dovoluje dodavatelům poskytovat kromě základní konfigurace též zdokonalenou OFDM“⁷. Tato norma už byla od začátku koncipována tak, aby byla zpětně kompatibilní s normou 802.11b. Z této skutečnosti ale i vyplývá, že pokud je v síti běžící na standardu 802.11g přítomno zařízení, které podporuje jen standard 802.11b, tak se výkon dané sítě velmi výrazně sníží. Tento standard byl

⁶ BRISBIN, S. *Wi-Fi: postavte si svou vlastní wi-fi síť*. Praha: Neocortex, 2003. 248 s. ISBN 80-291-8644-2.

⁷ BRISBIN, S. *Wi-Fi: postavte si svou vlastní wi-fi síť*. Praha: Neocortex, 2003. 248 s. ISBN 80-291-8644-2.

dodavateli a hlavně spotřebiteli, přijat velmi kladně. V létě roku 2003 se už prodávala většina tzv. tri-band zařízení, tedy zařízení podporujících všechny tři standardy.

Přes všechny kladné ohlasy na jeho zavedení standard 802.11b, trpí stejnými druhy rušení jako 802.11b, protože jak bylo zmíněno výše, pracuje na stejné přeplněné frekvenci 2,4 GHz. V této frekvenci totiž pracuje mnoho zařízení, jako například: mikrovlnné trouby, Bluetooth, domácí digitální bezšňůrové telefony nebo třeba baby monitory, které mohou vést k rušení sítě a tedy k rapidním ztrátám výkonu nebo dokonce k úplné ztrátě signálu. Navíc úspěch tohoto standardu vede k dalším problémům, v souvislosti s využitím v hustě zastavěných městských oblastech, kde se může na relativně malém prostoru vyskytovat velké množství domácích nebo firemních sítí, založených na tomto standardu. Aby se co nejvíce zabránilo narušení, existují tři (1, 6, 11, - rozdělení po 25 MHz), popřípadě čtyři (1, 5, 9, 13, - rozdělení po 20 MHz), nepřecházející se kanály, které lze využít.



Obr. 6.: Rozdělení kanálů (OFDM).⁸

Důvodem velkého úspěchu tohoto standardu je to, že navazuje na úspěšný standard 802.11b, a také skutečnost, že původní zařízení nezvládala zároveň standard 802.11b a

⁸ MyTselection [online]. 18.11.2009 [cit. 2010-05-09]. How to choose the right WiFi channel. Dostupné z WWW: < <http://mytselection.blogspot.com/2009/11/how-to-choose-right-wifi-channel.html> >

802.11a. Většina uživatelů vlastnících již starší přístroje, pracující na standardu 802.11b si při nákupu nějakého nového zařízení logicky koupila to, které bylo kompatibilní s jejich starším hardwarem.

1.2.5 Standard 802.11n

Standard 802.11n je nejnovějším schváleným standardem, upravujícím rychlost bezdrátového připojení. Tento standard si dává za cíl zvýšit přenosové rychlosti bezdrátové komunikace na rychlost srovnatelnou nebo vyšší, než je kabelový ethernet. Tento standard byl schválen v září roku 2009 a pracuje „v pásmech 2,4 GHz i 5 GHz, přičemž první z nich zajišťuje kompatibilitu s 802.11b/g. Pětigigahertzové pásmo naopak dosahuje vyšší reálné přenosové rychlosti. Dvoupásmové routery jsou bohužel výrazně dražší.“⁹

Je znám návrh standardu 802.11n, který počítá s rychlostí 600 Mbit/s ale zatím se teoretické rychlosti pohybují okolo 300 Mbit/s. Standardizační proces byl v případě této normy velmi komplikovaný. Ještě před samotným schválením (dokonce už od roku 2007) se objevovaly výrobky, které standard 802.11n podporovaly. Tyto výrobky však podporují první verzi standardu 802.11n tzv. Draft N. V dnešní době, by však většina přístrojů již měla podporovat konečnou verzi standardu – Draft 2.0.

Většina dnešních notebooků a dalších zařízení již podporuje standard 802.11n. Existují sice levnější modely, s podporou jen 802.11a/b/g, ale v dnešní době to již je spíše výjimkou.

Hlavním důvodem proč Standard 802.11n nabízí tak rapidní zvýšení přenosových rychlostí je využití technologie MIMO (Multiple-input multiple-output – více vstupů, více výstupů). MIMO je matematický model, pro komunikační systémy s více anténami. Teoretická stránka technologie je známa již velice dlouho. První myšlenky ohledně MIMO byly formulovány již v roce 1970. První dokumenty ohledně MIMO vytvořil v roce 1984 Jack Winters z Bell Laboratories, a o rok později Jack Salz, také z Bell Laboratories zveřejnil ohledně MIMO článek, založený na Wintersově výzkumu. Obecně technologie MIMO zefektivňuje bezdrátové datové přenosy po výkonnostní

⁹ NYGRÝN, Pavel. Wi-Fi zvládne každý!. *Computer*. 24. září 2009, 18/09, s. 6-8.

stránce. U 802.11n je MIMO použito společně s OFDM. MIMO není použito jen u Wi-Fi, ale také u mnoha dalších technologií je MIMO standardem nebo se jím v brzké době stane. Je to například WiMAX nebo HSDPA.



Obr. 7.:Bezdrátový router ASUS WL-500W podporující standard 802.11n.¹⁰

Zařízení (například routery) podporující standard 802.11n, lze velmi snadno rozeznat na první pohled od starších typů, podporujících jen 802.11a/b/g. Hlavním rozpoznávacím znakem je větší počet antén (obvykle tři, ale mohou být i dvě), právě

¹⁰ ASUSTeK computer Inc. [online]. 2009 [cit. 2010-05-09]. WL-500W. Dostupné z WWW: <http://usa.asus.com/product.aspx?P_ID=nrsjewu78wdDXMOA>.

kvůli použití technologie MIMO. Stejně jako v případě 802.11g, se při zapojení zařízení podporujícího nižší standard, než je 802.11n v síti rapidně sníží výkon. Tento problém je však aktuální hlavně u levnějších, jednopásmových zařízení (routerů). U dražších dvoupásmových zařízení, tento pokles výkonu není až tak rapidní.

1.2.6 Přehled dodatků ke standardu 802.11

IEEE 802.11 – Původní standard pro 2 Mbit/s rychlost s frekvencí 2.4 GHz (1997).

IEEE 802.11a – 54 Mbit/s, 5 GHz standard (1999, produkty od 2002).

IEEE 802.11b – Vylepšení 802.11 s podporou 5.5 a 11 Mbit/s (1999).

IEEE 802.11c – Bezdrátové přemostění (bridge) (2001).

IEEE 802.11d – Mezinárodní roamingový dodatek (2001).

IEEE 802.11e – Vylepšení QoS, včetně dlouhých (burst) paketů (2005).

IEEE 802.11F – Komunikace mezi bezdrátovými přístupovými body (2003). Stažen v březnu 2006.

IEEE 802.11g – 54 Mbit/s, 2.4 GHz standard (zpětně kompatibilní s 802.11b) (2003).

IEEE 802.11h – Správa spektra 802.11a (5 GHz) pro Evropu (2004).

IEEE 802.11i – Vylepšený autentizační a šifrovací algoritmus (WPA2) (2004).

IEEE 802.11j – Dodatek pro Japonsko - nová frekvenční pásma pro multimedia (2004).

IEEE 802.11k – Vylepšení správy rádiových zdrojů pro vysoké frekvence. (Navazuje na IEEE 802.11j).

IEEE 802.11l – Rezervováno a prozatím nebude použito.

IEEE 802.11m – Správa standardu - přenosové metody a drobné úpravy.

IEEE 802.11n – Vylepšení pro vyšší datovou propustnost.

IEEE 802.11o – Rezervováno a prozatím nebude použito.

IEEE 802.11p – Bezdrátový přístup pro pohyblivé prostředí (auta, autobusy, vlaky).

IEEE 802.11q – Rezervováno a nebude použito (aby se nepletlo s IEEE 802.1Q).

IEEE 802.11r – Rychlé přesuny mezi přístupovými body (roaming) (2008).

IEEE 802.11s – Samoorganizující se bezdrátové sítě. (ESS Mesh Networking).

IEEE 802.11T – Předpověď bezdrátového výkonu – testovací metody.

IEEE 802.11u – Spolupráce se sítí MIMO a dalších standardů (například mobilní sítě).

IEEE 802.11v – Správa bezdrátových sítí (konfigurace zařízení během připojení).

IEEE 802.11w – Chráněné servisní rámce.

IEEE 802.11x – Rezervováno a prozatím nebude použito.

IEEE 802.11y – Běh ve frekvenčním pásmu 3650 – 3700 MHz (veřejné pásmo v USA).

Poznámka: Pojem *802.11x* je neformálně používán k označení libovolného 802.11 standardu. (Standard IEEE 802.1X pro řízení přístupu k síti a, založený na autentizaci a filtrování portů, bývá běžně nesprávně označován jako 802.11x.)

802.11F a 802.11T jsou samostatné dokumenty, a nejsou to tedy dodatky k IEEE 802.11 standardu. Proto obsahují velké písmeno.¹¹

¹¹ *Wi-Fi síť Praha* [online]. 2008 [cit. 2010-05-09]. Wi-Fi standard IEEE 802.11. Dostupné z WWW: <<http://prahawifi.cz/wifi-standard-ieee-80211/>>.

1.3 Zabezpečení bezdrátových sítí

1.3.1 Filtrování MAC adres

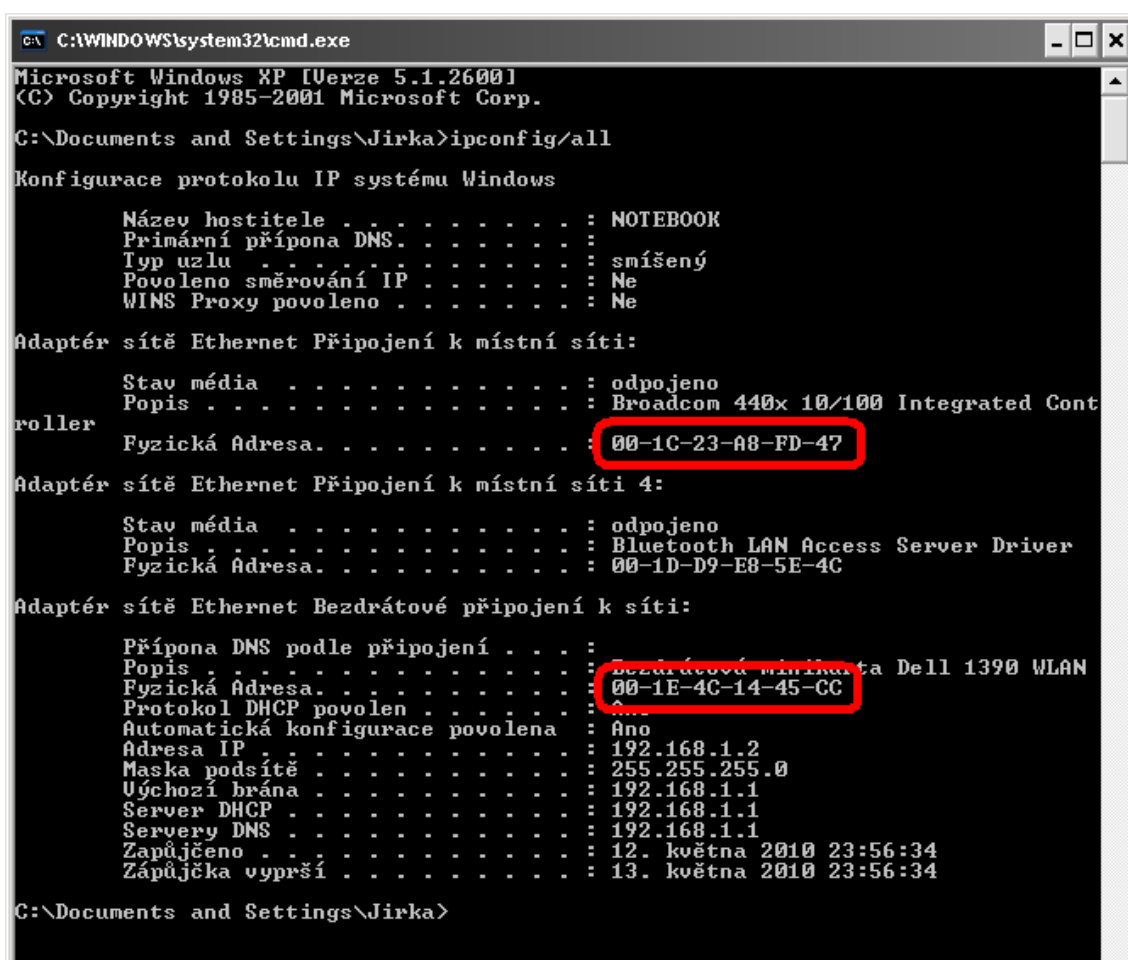
Filtrování MAC adres, neboli filtrování fyzických adres je jedna z nejjednodušších forem zabezpečení bezdrátové sítě – a také velmi nespolehlivá. „MAC adresa (zkratka z Media Access Control) je jedinečný identifikátor síťového zařízení, který používají různé protokoly, druhé (spojové) vrstvy OSI. Je přiřazována síťové kartě NIC, bezprostředně při její výrobě (u starších karet je přímo uložena do EEPROM paměti), nicméně ji lze dnes u moderních karet dodatečně změnit. Ethernetová MAC adresa se skládá ze 48 bitů a podle standardu, by se měla zapisovat jako tři skupiny, čtyř hexadecimálních čísel (např. 0123.4567.89AB), mnohem častěji se ale píše jako šestice, dvojciferných hexadecimálních čísel, oddělených pomlčkami nebo dvojtečkami (např. 01-23-45-67-89-AB nebo 01:23:45:67:89:AB).“¹²

Wireless - Access Control				
Access Control allows you to block the access from certain wireless stations or to bypass access from certain wireless stations only. In Accept mode, ASUS Wireless Router will only accept wireless access from stations with MAC address in the control list. In Reject mode, ASUS Wireless Router will reject wireless access from stations with MAC address in the control list.				
MAC Access Mode:	Accept			
Access Control List				
Add Del				
<table border="1"><thead><tr><th>MAC Address</th></tr></thead><tbody><tr><td>002655f52069</td></tr><tr><td>001E4c1445cc</td></tr></tbody></table>		MAC Address	002655f52069	001E4c1445cc
MAC Address				
002655f52069				
001E4c1445cc				

Obr. 8.: Nastavení filtru MAC adres u bezdrátového routeru ASUS WL-520gC.

¹² *Linux E X P R E S* [online]. 2007 [cit. 2010-05-13]. Domácí počítačová síť - 2. Dostupné z WWW: <<http://www.linuxexpres.cz/praxe/domaci-pocitacova-sit-2>>

Každý packet, který je součástí komunikace mezi jednotlivými počítači, v rámci Wi-Fi sítě je vybaven právě dvěma MAC adresami. Adresou vysílajícího prvku sítě a adresou prvku, pro který je packet určen. Většina (prakticky všechny), z dnešních Wi-Fi routerů, podporuje funkci filtrování MAC adres. Zjednodušeně to funguje tak, že se v nastavení routeru zadají adresy zařízení, které se chtějí do sítě připojovat pomocí Wi-Fi. Většina routerů podporuje dva režimy – Accept (v tomto režimu jsou akceptovány jen packety, které jsou uvedeny v seznamu) a Reject (v tomto režimu jsou akceptovány všechny přichozí packety kromě těch, co jsou v seznamu). Pokud má tedy router nastavené filtrování MAC adres a je v režimu Accept, komunikuje jen se zařízeními, která jsou v seznamu povolena a packety od ostatních (nepovolených) zařízení odhazuje a nebere na ně zřetel.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Verze 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Jirka>ipconfig/all

Konfigurace protokolu IP systému Windows

    Název hostitele . . . . . : NOTEBOOK
    Primární přípona DNS . . . . . : 
    Typ uzlu . . . . . : smíšený
    Povoleno směrování IP . . . . . : Ne
    WINS Proxy povoleno . . . . . : Ne

Adaptér sítě Ethernet Připojení k místní síti:

    Stav média . . . . . : odpojeno
    Popis . . . . . : Broadcom 440x 10/100 Integrated Cont
    Fyzická Adresa. . . . . : 00-1C-23-A8-FD-47

Adaptér sítě Ethernet Připojení k místní síti 4:

    Stav média . . . . . : odpojeno
    Popis . . . . . : Bluetooth LAN Access Server Driver
    Fyzická Adresa. . . . . : 00-1D-D9-E8-5E-4C

Adaptér sítě Ethernet Bezdrátové připojení k síti:

    Přípona DNS podle připojení . . . . : 
    Popis . . . . . : Bezdrátová mini-karta Dell 1390 WLAN
    Fyzická Adresa. . . . . : 00-1E-4C-14-45-CC
    Protokol DHCP povolen . . . . . : Ano
    Automatická konfigurace povolena . . : Ano
    Adresa IP . . . . . : 192.168.1.2
    Masky podsítě . . . . . : 255.255.255.0
    Účchozí brána . . . . . : 192.168.1.1
    Server DHCP . . . . . : 192.168.1.1
    Servery DNS . . . . . : 192.168.1.1
    Zapůjčeno . . . . . : 12. května 2010 23:56:34
    Zápujčka vyprší . . . . . : 13. května 2010 23:56:34

C:\Documents and Settings\Jirka>
```

Obr. 9.: Zjištění MAC adresy PC pomocí příkazu ipconfig/all.

Jak již jsem psal výše, spolehlivost tohoto zabezpečení je velmi nízká. Je to z toho důvodu, že je sice omezena komunikace jen na daný seznam zařízení, které se k síti připojují, ale problém je v tom, že komunikace mezi povolenými zařízeními není nijak šifrována nebo skryta. Z toho vyplývá, že pokud se chce útočník dostat do sítě zabezpečené tímto způsobem, není nic jednoduššího, než odchytit pár paketů při komunikaci povoleného zařízení s routerem a pomocí softwaru z nich dostat MAC adresu, vysílajícího zařízení. Potom mu už jen stačí změnit MAC adresu svého zařízení na adresu zjištěnou a útočník má přístup do bezdrátové sítě umožněn. Tento typ zabezpečení je tedy velmi jednoduché prolomit. Ve většině případů se buď nepoužívá, nebo je použito v kombinaci s nějakým jiným zabezpečením, jako je například WEP nebo ještě lépe WPA nebo WPA2.

Klasickým útokem na toto zabezpečení je tzv. MAC Attack. „Adresa MAC pro připojení na přístupový bod se zjišťuje stejně, jako se dekoduje WEP klíč. Pokud není v síti WEP aktivováno, stačí útočnickovi zachytávat komunikaci mezi přístupovým bodem a klientem a vyhledat si hlavičku MAC adresy a tu si pak přečíst. Pokud je WEP používán, musí útočník nejdříve dekodovat WEP, v tomto případě mu postačuje i offline analýza zachycených datových rámců.

V okamžiku, kdy útočník získá MAC adresu, může ji podstrčit své klientské kartě a vystupovat jako oprávněný uživatel.“¹³

MAC útokům lze předejít použitím zabezpečení, například na bázi VPN (Virtuální privátní síť), nebo autentizačních mechanismů, jako je například 802.1x.

1.3.2 Skrytí SSID sítě

SSID neboli Service Set Identifier jednoznačné pojmenování bezdrátové sítě, které se každých pár sekund vysílá v tzv. beacon frame (majákový rámeček). Toto pojmenování bývá využíváno při veškeré komunikaci jednotlivých zařízení v síti. Pokud se SSID neshoduje, je komunikace odmítnuta. SSID je vlastně řetězec alfanumerických znaků, o

¹³ ZANDL, P. *Bezdrátové sítě WiFi: praktický průvodce*. Vyd. 1. Brno: Computer Press, 2003. 190 s. ISBN 80-7226-632-2.

maximální délce 32 oktetů. Stejně jako filtrování MAC adres, je skrytí SSID velmi jednoduchou formou zabezpečení, kterou je není vůbec těžké prolomit.

Wireless - Advanced	
This section allows you to set up additional parameters for wireless. But default values are recommended.	
Enable AfterBurner?	Enabled v
Hide SSID:	☐ Yes ☒ No
Set AP Isolated?	☐ Yes ☒ No
Data Rate(Mbps):	Auto v
Basic Rate Set:	All v
Fragmentation Threshold:	2346
RTS Threshold:	2347

Obr. 10.: Nastavení skrytí SSID u bezdrátového routeru ASUS WL-520gC.

V případě nevysílání SSID, se v závislosti na používaném softwaru pro bezdrátové připojení, síť buď vůbec nezobrazuje, nebo se zobrazuje jako síť bez názvu.

Postup při prolomení tohoto zabezpečení je obdobný, jako v případě filtrování MAC adres. Kdykoliv, se totiž někdo přihlásí do sítě zabezpečené tímto způsobem, tak vysílá nijak nešifrované SSID aby se mohl připojit. Útočníkovi pak už jen stačí, za pomoci specializovaného softwaru odchytil tento řetězec znaků a poté se už může jednoduše, do takto zabezpečené sítě připojit, bez jakékoliv omezení. Podobně jako u filtrování MAC adres se buď tento typ zabezpečení vůbec nepoužívá, nebo se používá v kombinaci s nějakým dalším, vyspělejším zabezpečením.

1.3.3 WEP

Šifrování WEP se už od počátku součástí standardu 802.11. „Protokol WEP (Wired Equivalent Privacy) pracuje jako volitelný doplněk k 802.11 (Wi-Fi Alliance pro certifikaci Wi-Fi produktů WEP požaduje povinně), pro řízení přístupu k síti a zabezpečení přenášených dat. WEP byl původně určený pro dosažení takové bezpečnosti komunikace v bezdrátové síti, jaká odpovídá bezpečnosti v tradičních LAN

(jak ostatně jeho název napovídá), ale ve výsledku tato očekávání nesplnil. Měl sloužit jak autentizaci, tak pro ochranu přenášených dat šifrováním se stejným tajným klíčem. Norma však nespecifikuje, jak se klíče distribuují.

Authentication Method	Shared Key ▼
WPA Encryption:	TKIP+AES ▼
WPA Pre-Shared Key:	
WEP Encryption:	WEP-64bits ▼
Passphrase:	WEP-64bits WEP-128bits
WEP Key 1 (10 or 26 hex digits):	4776C66C27
WEP Key 2 (10 or 26 hex digits):	A02400A5BA
WEP Key 3 (10 or 26 hex digits):	63DC84011B
WEP Key 4 (10 or 26 hex digits):	4AB8316903
Key Index:	1 ▼
Network Key Rotation Interval:	0

Obr. 11.: Nastavení zabezpečení WEP u bezdrátového routeru ASUS WL-520gC.

WEP nemusí být nutně použit pro autentizaci i šifrování; lze jej využít jen pro šifrování a autentizaci provést jinými metodami, což je vzhledem k slabinám autentizace WEP dokonce výhodnější.¹⁴ Hlavními vlastnostmi WEP jsou tedy: jednostranná autentizace, šifrování v dnešní době už ne příliš silnou proudovou šifrou RC4, s délkou klíče pouze 40 bitů. Slabinami WEP jsou snadno narušitelné statické klíče, které jsou náchylné k řadě útoků. WEP byl v době aktuality standardu 802.11b, spolu s skrýváním SSID hlavním zabezpečením. V dnešní době je však překonán i když nabízí mnohem lepší zabezpečení, v porovnání třeba s filtrováním MAC adres nebo skrýváním SSID samotným.

¹⁴ PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace : Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G*. Brno : Computer Press, 2005. 186 s.

„Všechny sítě 802.11 mají zabudovaný protokol WEP (Wired Equivalent Privacy). WEP používá symetrický postup šifrování, kdy pro šifrování a dešifrování se používá stejný algoritmus i stejný klíč. Autentizace v rámci WEP je považována za velice slabou až nulovou. 40bitový uživatelský klíč pro autentizaci je statický a stejný pro všechny uživatele dané sítě (sdílený klíč, shared secret) klienti jej používají společně se svou adresou MAC pro autentizaci vůči přístupovému bodu (ve skutečnosti se ověřuje totožnost síťové karty, nikoli samotné osoby uživatele). Autentizace se provádí pouze jednostranně, přístupový bod se neautentizuje.

V 802.11 není definován mechanismus managementu WEP klíčů, který by se staral o automatickou distribuci klíčů a jejich obnovu.

Šifrování přenášených dat ve WEP se provádí 64bitovým klíčem, který je složen z uživatelského klíče a dynamicky se měnícího vektoru IV (Initialization Vector) v délce 24 bitů, nebo lépe 128bitovým klíčem (sdílený klíč pak má délku 104 bitů, vektor má délku 24 bitů). IV se posílá otevřené formě a mění se obvykle s každým paketem, takže výsledné šifrování je jedinečné pro každý jednotlivý paket ve WLAN. WEP používá šifrovací algoritmus RC4. Bezpečnost sítě s WEP lze narušit jak mechanicky (krádeží jednoho z koncových zařízení s příslušnou WiFi kartou), tak odposlechem.

Pro středně zkušené a vybavené narušitele není – s trochou trpělivosti – obtížné WEP porazit.“¹⁵

WEP Cracking neboli „luštění WEP je oblíbenou metodou útočníků. K rozluštění klíče je zapotřebí mezi 5 a 10 miliony paketů, a útočník spoléhá na to, že po celou dobu kdy je bude zachytávat WEP klíč nezměníte. Útočníci mají k dispozici open source programy jako je AirSnort nebo WEPCrack a stačí jim zachytávat komunikaci mezi přístupovým bodem a klientem“¹⁶

¹⁵ PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace : Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G*. Brno : Computer Press, 2005. 186 s.

¹⁶ ZANDL, P. *Bezdrátové sítě WiFi: praktický průvodce*. Vyd. 1. Brno: Computer Press, 2003. 190 s. ISBN 80-7226-632-2.

Obranou může být použití dalšího šifrování, popřípadě autentizačních mechanismů například pomocí VPN a 802.1x.

1.3.4 WPA

WPA je zkratka pro Wi-Fi Protected Access, což je česky Wi-Fi chráněný přístup nebo Wi-Fi, s chráněným přístupem a je nástupcem WEP. Hlavním cílem bylo poučit se z nedostatků WEP a nabídnout kvalitnější a komplexnější zabezpečení pro bezdrátovou komunikaci. Původně se tento návrh jmenoval WEP2, ale nakonec byl změněn na WPA. „Podle zákulisních údajů, pocházejících z Wi-Fi aliance se údajně říkalo, že „když se loď potopí, tak tu novou nepojmenujete Titanic 2“. 31. října 2002 ohlásila Wi-Fi aliance protokol WPA, což bylo v zásadě kompromisní řešení, protože některé části specifikace 802.11i už byly hotovy (například 802.1x a TKIP tedy Temporal Key Integrity Protocol), zatímco jiné ještě ne (například AES, Advanced Encryption Standard a zabezpečená deautentizace a disasociace)

Logika, kterou se Wi-Fi aliance řídila, byla prostá: Nemůžeme čekat do doby, než dojde k ratifikaci 802.11i, což se stane přinejlepším za rok nebo dva, takže vezmeme to, co je hotovo a vydáme to ihned. WPA je tak podmnožinou 802.11i, kterou lze implementovat prostřednictvím aktualizace softwaru a firmwaru. Řeší jak šifrování, tak řízení přístupu (802.1x).

Z bezpečnostního pohledu mají tyto technologie značný význam, protože řeší řadu slabín a bezpečnostních děr protokolů WEP a 802.11¹⁷

Ve standardu WPA je vylepšen šifrovací algoritmus. Další výhodou je dobrá správa šifrovacích klíčů, což umožňuje interní změnu šifrovacího klíče bez toho, aby někdo nový klíč zjistil. Ke změnám šifrovacích klíčů dochází v předem daných časových úsecích, to znamená že případný útočník má mnohem méně času na zjištění klíče a jeho použití.

¹⁷ BARKEN, L. *Wi-Fi: jak zabezpečit bezdrátovou síť*. Vyd. 1. Brno: Computer Press, 2004. 174 s. ISBN 80-251-0346-3.

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	PW: Hex	PW: ASCII
	00:0B:06:BB:8F:73			Mon Aug 30 12:57:21 2004	00:00:00	1	0	0			
	00:0C:E5:0E:74:1B	Cox-Hospitality		Mon Aug 30 12:58:01 2004	00:00:00	6	9	0	0		
	02:04:23:D7:55:21	Cox-Hospitality		Mon Aug 30 12:57:21 2004	00:00:00	6	1	0	0		
	00:0B:06:BA:D8:9D	Cox-Hospitality		Mon Aug 30 12:57:34 2004	00:00:00	6	3	0	0		
	00:0B:06:BC:83:2D	Cox-Hospitality	Y	Mon Aug 30 12:59:05 2004	AA:AA:03	11	662	420	0		
	00:0B:06:BC:7D:75	Cox-Hospitality		Mon Aug 30 12:57:22 2004	00:00:00	11	1	0	0		
	00:0C:E5:0E:67:13	Cox-Hospitality	Y	Mon Aug 30 12:58:15 2004	AA:AA:03	1	17	6	0		
	00:0B:06:BC:23:B7			Mon Aug 30 12:57:24 2004	00:00:00	2	0	0	0		
	00:0B:06:BB:EE:35	Cox-Hospitality		Mon Aug 30 12:58:41 2004	00:00:00	11	3	0	0		
	00:0B:06:BC:17:75	Cox-Hospitality	Y	Mon Aug 30 12:57:27 2004	E0:E0:03	1	4	2	0		
	00:0B:06:BA:EB:15	Cox-Hospitality		Mon Aug 30 12:58:19 2004	00:00:00	1	3	0	0		
	00:0B:06:BB:EA:57	Cox-Hospitality		Mon Aug 30 12:57:24 2004	00:00:00	1	1	0	0		
	00:0B:06:BA:E1:73	CoxHospitality	Y	Mon Aug 30 12:58:19 2004	AA:AA:03	1	13	3	0		
	00:0B:06:BA:D2:EB		Y	Mon Aug 30 12:58:19 2004	AA:AA:03	6	6	6	0		
	00:0B:06:BC:89:57			Mon Aug 30 12:57:25 2004	00:00:00	1	0	0	0		
	00:0B:06:BA:E1:97	Cox-Hospitality	Y	Mon Aug 30 12:59:05 2004	AA:AA:03	11	54	4	0		
	00:0B:06:BB:99:1B	Cox-Hospitality	Y	Mon Aug 30 12:58:56 2004	E0:E0:03	11	8	1	0		
	00:0B:06:BB:98:DF	Cox-Hospitality	Y	Mon Aug 30 12:57:26 2004	AA:AA:03	11	5	2	0		
	00:0B:06:BC:8C:69	Cox-Hospitality		Mon Aug 30 12:58:18 2004	00:00:00	6	4	0	0		
	00:0B:06:BB:21:93	Cox-Hospitality		Mon Aug 30 12:58:18 2004	00:00:00	6	4	0	0		
	00:02:2D:6D:DE:B6	MANDALAY		Mon Aug 30 12:58:15 2004	00:00:00	1	10	0	0		
	00:0B:06:BB:98:D3			Mon Aug 30 12:58:40 2004	00:00:00	2	0	0	0		
	00:0B:06:BB:2C:7F	Cox-Hospitality		Mon Aug 30 12:58:19 2004	00:00:00	1	10	0	0		
	00:02:2D:6D:DE:B0	MANDALAY		Mon Aug 30 12:58:09 2004	00:00:00	3	5	0	0		
	00:0B:06:BA:C3:9D			Mon Aug 30 12:57:58 2004	00:00:00	1	0	0	0		
	00:0B:06:BB:21:E7	Cox-Hospitality	Y	Mon Aug 30 12:58:20 2004	AA:AA:03	6	22	11	0		
	00:02:2D:6D:DE:F9	MANDALAY		Mon Aug 30 12:58:12 2004	00:00:00	6	7	0	0		
	00:0B:06:66:5C:79			Mon Aug 30 12:58:13 2004	00:00:00	6	0	0	0		
	00:0B:06:BA:C5:5F			Mon Aug 30 12:58:13 2004	00:00:00	2	0	0	0		
	00:0B:06:BA:E6:E3	Cox-Hospitality		Mon Aug 30 12:58:19 2004	00:00:00	1	8	0	0		
	00:0B:06:BA:E0:CB	Motorola		Mon Aug 30 12:58:13 2004	00:00:00	1	2	0	0		
	00:0B:06:BC:77:1B	Cox-Hospitality		Mon Aug 30 12:58:15 2004	00:00:00	1	3	0	0		
	00:0B:06:BB:9D:35	Cox-Hospitality		Mon Aug 30 12:58:13 2004	00:00:00	1	1	0	0		
	00:0B:06:BA:E6:AD	Cox-Hospitality		Mon Aug 30 12:58:17 2004	00:00:00	1	3	0	0		
	00:0B:06:BB:2C:D9			Mon Aug 30 12:58:14 2004	00:00:00	1	0	0	0		
	00:0B:06:BB:A5:3F	Cox-Hospitality	Y	Mon Aug 30 12:59:05 2004	AA:AA:03	11	247	124	0		
	00:0B:06:BC:46:CD	Cox-Hospitality		Mon Aug 30 12:58:15 2004	00:00:00	1	2	0	0		

Obr. 12.: Okno programu AirSnort.

Pro použití WPA je nutný dostatečně výkonný hardware, ale i aktualizovaný software. Někdy se stávalo (v dnešní době je to již spíše výjimkou, ale v minulosti bylo možné na tento problém narazit), že daný hardware nebyl dostatečně výkonný a standardy WPA nebylo možné podporovat. WPA je nemožné používat zároveň s WEP. V síti mohou být přítomna buď zařízení zabezpečená pomocí WPA nebo WEP. Z toho vyplývá, že pokud chcete v síti použít zabezpečení WPA, je nutné aby veškerá zařízení v síti tento standard podporovala.

Channel	Auto v
Wireless Mode	54G Only v ☐ 54g Protection
Authentication Method	WPA-Personal v
WPA Encryption:	TKIP+AES v
WPA Pre-Shared Key:	
WEP Encryption:	None v
Passphrase:	
WEP Key 1 (10 or 26 hex digits):	
WEP Key 2 (10 or 26 hex digits):	
WEP Key 3 (10 or 26 hex digits):	

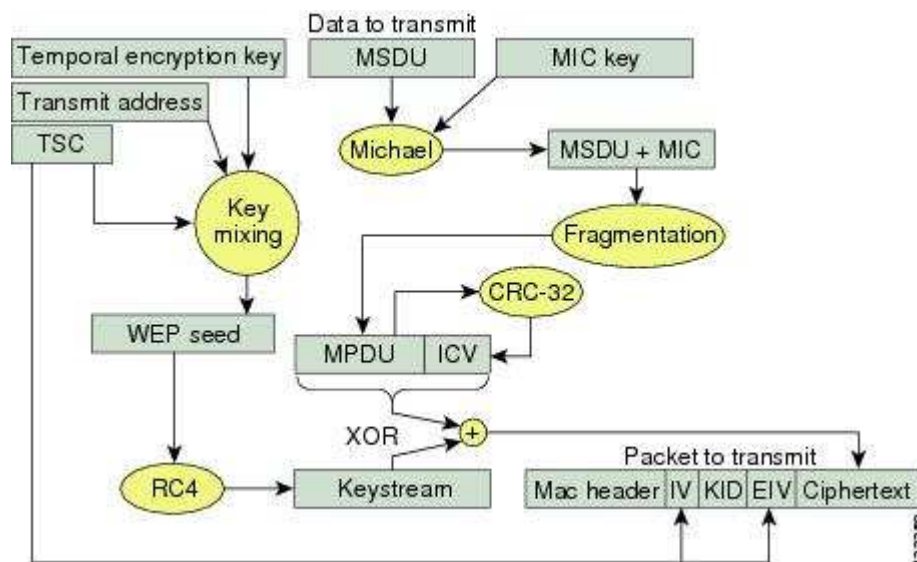
Obr. 13.: Nastavení zabezpečení WPA u bezdrátového routeru ASUS WL-520gC.

Oproti WEP ze kterého vychází, WPA se snaží řešit největší bezpečnostní díry v rámci standardu 802.11 i samotného WEP. Lze zmínit pár nevýhod WEP a jejich řešení ve WPA. WEP používá 24bitový inicializační vektor, který slouží jako část inicializačního údaje generátoru RC4. Tento inicializační vektor nebo spíše jeho hodnota, by měla být použita právě jednou, aby se zamezilo případným bezpečnostním rizikům. Často však dochází opakování hodnoty inicializačního vektoru, protože k vyčerpání všech kombinací v 24bitovém prostoru dochází v silném provozu, během několika hodin. Jakmile však dojde k opětovnému použití inicializačního vektoru, stává se celý systém velmi zranitelný vůči útokům na šifrovací sekvenci a také vůči opakovacím útokům. „Útok na šifrovací sekvenci je založen na základní skutečnosti, že XOR dvou zašifrovaných textů dává stejný výsledek, jako XOR dvou přímých textů. Opakovací útok pak vezme známou zašifrovanou sekvenci a použije ji k podvržení nových paketů. Opakovací útoky jsou možné díky tomu, že WEP akceptuje libovolné hodnoty IV.

Dalším významným problémem protokolu WEP, popsaným v FMS a využitým v programech jako je AirSnort, WEPCrack a dweputils je algoritmus pro plánování klíče. Díky tomuto problému je možné rozluštit hodnotu klíče, po zachycení dostatečného objemu šifrovaných dat.

A konečně je možné technikou „přehazování bitů“ zmást funkci pro kontrolu integrity, která používá 32bitovou hodnotu CRC. Útočník může modifikovat přenášený paket a změnit bity kontrolního součtu tak, že změna nebude detekovatelná.

WPA řeší tyto problémy prostřednictvím mechanismů TKIP a 802.1x.



Obr. 14.: Mechanismus TKIP.¹⁸

TKIP řeší následující slabiny:

- Útok opakováním – možnost opakovaného použití hodnoty IV.
- Podvržení – ICV používá 32bitovou lineární hodnotu CRC, s níž lze manipulovat.
- Útoky založené na kolizi – kolize IV.
- Útoky na slabé klíče – šifra RC4 je napadnutelná útokem FMS (AirSnort, WEPCrack, dweputils a další)

¹⁸ Cisco Systems, Inc [online]. 2010 [cit. 2010-05-25]. Cisco Unified Wireless Network Architecture - Base Security Features. Dostupné z WWW:
<http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch4_Secu.html>.

Protokol 802.1x pak řeší tyto slabiny:

- Chybějící správa klíčů.
- Chybějící podpora „pokročilých“ autentizačních metod (tokeny, čipové karty, certifikáty, biometriky, jednorázová hesla a podobně).
- Chybějící identifikace a autentizace uživatelů.
- Chybějící centralizovaná autentizace a autorizace.

První produkty odpovídající standardu WPA se na trhu objevily v květnu 2003. Vylepšení nabízená protokolem WPA se ovšem nedají použít pro sítě typu ad-hoc a fungují pouze v sítích BSS/ESS s instalovanými AP.

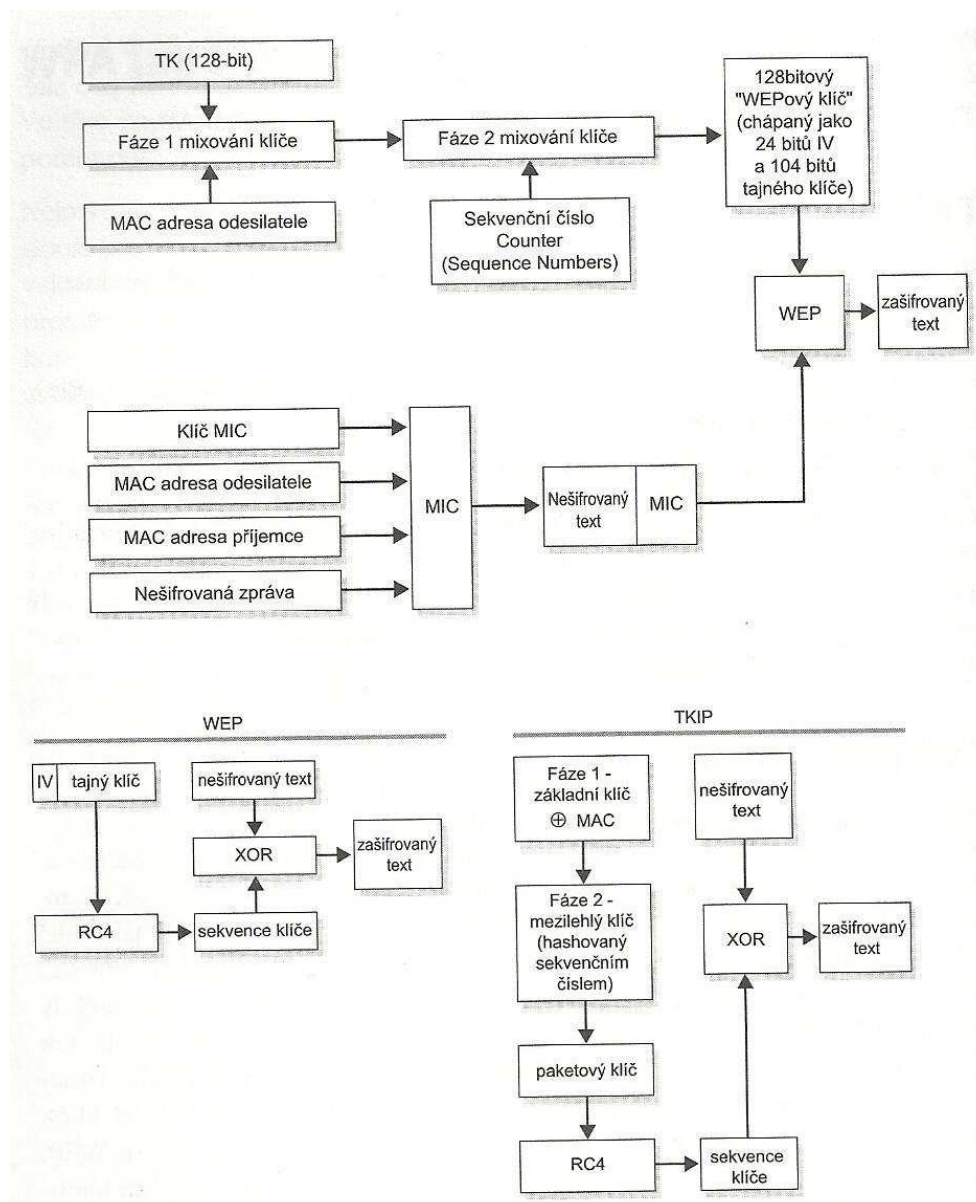
Mechanismus TKIP navíc zlepšuje šifrování pomocí tří hlavních prvků:

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

V zásadě představuje TKIP pouze dočasnou opravu protokolu WEP, kterou lze implementovat jednoduchým upgradem softwaru/firmwaru. Kvůli zachování zpětné kompatibility s velkým počtem stávajících instalovaných hardwarových zařízení byly při jeho návrhu učiněny různé kompromisy.¹⁹

TKIP klient začíná dvěma klíči 128bitovým šifrovacím klíčem a 64bitovým klíčem, pro zajištění integrity. Tyto klíče se získávají bezpečnými mechanismy při první komunikaci protokolem 802.1x. Označení prvního, šifrovacího klíče je Temporary Key neboli TK. Označení druhého klíče je poté Message Integrity Code, neboli MIC.

¹⁹ BARKEN, L. *Wi-Fi: jak zabezpečit bezdrátovou síť*. Vyd. 1. Brno: Computer Press, 2004. 174 s. ISBN 80-251-0346-3.



Obr. 15.: Kódování pomocí TKIP, porovnání šifrování ve WEP a ve WPA.²⁰

Proces ověření probíhá tak, že se provede XORování hodnoty TK a MAC adresy odesílatele. Takto vzniká tzv. First Phase Key (mezilehlý klíč). Pro vytvoření Second Phase Key se používá tzv. mixování First Phase Key, se sekvenčním číslem a výstupem je standardní 128bitový WEP klíč. Zbytek procesu je prakticky stejný, jako v zabezpečení WEP. Hlavním bezpečnostním posílením oproti WEP je to, že díky první

²⁰ BARKEN, L. *Wi-Fi: jak zabezpečit bezdrátovou síť*. Vyd. 1. Brno: Computer Press, 2004. 174 s. ISBN 80-251-0346-3.

fázi procesu všichni klienti už nepoužívají stejný WEP klíč. Druhá fáze má za následek neexistenci korelace, mezi hodnotou inicializačního vektoru a samotným klíčem. Dosahuje se toho pomocí Fiestelovy šifry, kterou navrhli Doug Whiting a Ron Rivest. Díky této skutečnosti, nelze využít programů jako je AirSnort, WEPCrack a dweputils.

„Připomeňme si, že problém původního návrhu protokolu WEP spočíval v tom, že hodnota IV se jednoduše připojila k tajnému klíči a předala generátoru RC4. U TKIP první fáze zajistí, že každý klient používá jiný mezilehlý klíč. Ve druhé fázi se tento klíč mixuje se sekvenčním číslem a teprve tento výsledek se následně předává generátoru RC4. Jak můžeme vidět, jde o propracovanější postup, než je prosté připojení hodnoty IV k tajnému klíči. Díky tomuto mechanismu tak TKIP odstraňuje nevhodnou implementaci použití RC4 ve WEPu“²¹ (obrázek 15).

Dále je důležitý mechanismus pojmenovaný Michael což je vlastně funkce pro kontrolu integrity. Ta funguje následovně: „Namísto jednoduché 32bitové hodnoty CRC se v TKIP ke kontrole integrity používá funkce Michael, jednocestná hashovací funkce, navržená Nielsem 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.

Problém s kolizemi IV řeší TKIP pomocí dvou jednoduchých pravidel. Prostor inicializačního vektoru se zvětšil z 24 bitů na 48 bitů. Při rychlosti 54 Mbps to znamená, že vyčerpání stavového prostoru bude trvat přes 1000 let. A zadruhé TKIP nařizuje, že hodnota IV roste inkrementálně od nuly a hodnoty mimo pořadí se ignorují.

Z pohledu bezpečnosti znamená rozšíření prostoru IV (respektive sekvenčního čísla) to, že se eliminují kolize IV a na nich založené útoky.

²¹ BARKEN, L. *Wi-Fi: jak zabezpečit bezdrátovou síť*. Vyd. 1. Brno: Computer Press, 2004. 174 s. ISBN 80-251-0346-3.

Jak bylo řečeno, TKIP zajišťuje i distribuci klíčů v infrastruktuře protokolu 802.11x (jako je například server RADIUS). Ne všichni domácí uživatelé mají tuto infrastrukturu k dispozici, takže aby mohli využívat šifrovacích funkcí TKIP, zavádí WPA speciální režim, označovaný jako režim s předsdíleným klíčem (Pre-Shared Key, PSK).

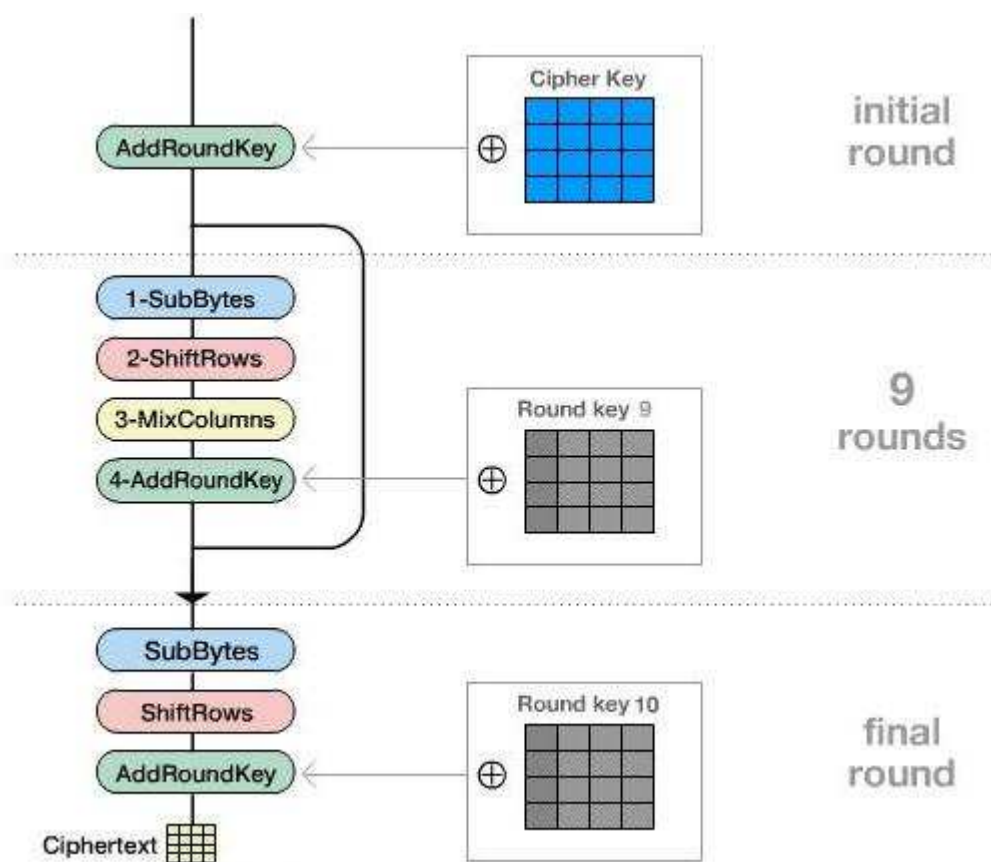
V tomto režimu musí všichni uživatelé na všech klientech a AP nastavit sdílenou tajnou hodnotu, takzvaný „master key“. Je to trochu podobné tomu, když se u protokolu WEP všude nastavoval WEPový klíč. Na rozdíl od WEPu však TKIP používá tento klíč pouze jako výchozí hodnotu, z níž se matematicky odvodí potřebné šifrovací klíče. Na rozdíl od WEPu, kde se stejný klíč používal stále dokola, provádí TKIP změnu šifrovacích klíčů, takže je zaručeno, že stejný klíč nebude nikdy použit dvakrát.“²²

WPA i přes své nesporné výhody oproti WEP je stále jen mezistupněm a z tohoto důvodu není tak dokonalé, jak by mohlo být. WPA bylo navrženo pouze jako dočasné opatření, před vydáním standardu 802.11i. V dnešní době je WPA již nahrazeno vylepšeným nástupcem WPA2. Přesto jej ale nesmíme odsuzovat. Ve své době dokázalo mnohem lépe zabezpečit bezdrátovou síť, než WEP. Důležité je také vzít v úvahu nutnost zpětné kompatibility, která výrazně snižuje možnosti zabezpečení a skoro doslova svazuje standardu WPA ruce – tímto způsobem byla omezena možnost navrhnout ideální řešení, protože většina zařízení existujících v té době, neměla vhodný hardware a dostatečný výkon CPU, nutný k podpoře výkonnějších šifrovacích programů. I když WPA bylo podrobena mnohem lepší kryptoanalýze než WEP, stále z něj vychází, k šifrování stále využívá šifru RC4, která je použita ve WEP. Přesto WPA těchto omezených možností, které má, využívá co možná nejlépe a z tohoto důvodu je mnohem bezpečnější, než jeho předchůdce, který trpěl mnoha neduhy. Dalším důkazem který říká, že WPA bylo ve své době (a i dnes je v podstatě velmi dobře využitelný bezpečnostní systém, pro zařízení s nižším výkonem, jako jsou třeba smartphony), velmi kvalitní zabezpečení je to, že nástupce je pojmenován WPA2.

²² BARKEN, L. *Wi-Fi: jak zabezpečit bezdrátovou síť*. Vyd. 1. Brno: Computer Press, 2004. 174 s. ISBN 80-251-0346-3.

1.3.5 WPA2

WPA2 neboli standard 802.11i je přímým nástupcem WPA. Ve WPA byla implementována jen část práce pracovní skupiny 802.11i a proto nebyla úplně přesně to, co tato pracovní skupina zamýšlela. Standard 802.11i – WPA2 byl schválen v roce 2004 a přináší konečně velmi robustní zabezpečení bezdrátové sítě. Hlavní a asi nejdůležitější komponentou standardu 802.11i je využití šifry AES (tato část 802.11i při vydávání WPA v polovině roku 2003 ještě nebyla hotova). Ve specifikaci 802.11i je AES povinná, ale TKIP je pouze volitelné.



Obr. 16.: Průběh šifrování pomocí AES.²³

Zkratka AES znamená Advanced Encryption Standard, což v překladu znamená vylepšený kódovací standard. Původně vychází z šifry DES (Data Encryption

²³ Computer Science at Boston College [online]. 2010 [cit. 2010-05-28]. AES encryption flash animation. Dostupné z WWW: <http://www.cs.bc.edu/~straubin/cs381-05/blockciphers/rijndael_ingles2004.swf>

Standard), což byla symetrická šifra, která byla vyvinuta v 70. letech v USA a v roce 1977 byla schválena jako standard pro šifrování v civilních státních organizacích v USA a následně pronikla i do soukromého sektoru. Je založena na algoritmu se symetrickým klíčem, který je 56bitový. V dnešní době je tento algoritmus považován za nepoužitelný v zabezpečení, protože se zvyšováním výpočetního výkonu počítačů, je 56bitová šifra prostě nedostačující. Dokazuje to i skutečnost, že poprvé byla tato šifra prolomena 17.6.1997 a dokonce v lednu 1999 byla tato šifra prolomena za pouhých 22 hodin a 15 minut útoku brutální silou (útok, který zkouší jednu kombinaci klíče za druhou).

Samotná AES je však mnohem propracovanější, než DES. Je stejně jako DES symetrická, ale může využívat buď 128bitového, 192bitového nebo 256bitového klíče, čímž je oproti DES nebo RC4 mnohem robustnější a výkonnější. V současné době dokonce není veřejně znám žádný případ plného prolomení této ochrany dat.

„AES je šifra odpovídající americkému federálnímu standardu FIPS (Federál Information Processing Standards) která byla navržena jako náhrada RC4. Samotnému přijetí šifry AES americkou vládou předcházela 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 bloky 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 802.1x. V terminologii CCMP se 48bitová hodnota IV označuje jako „číslo paketu“ (PN).

Stejně jako TKIP i CCMP obsahuje algoritmus MIC zajišťující, že nedošlo k modifikaci přenášených dat. Nicméně mechanismus MIC v CCMP funguje jinak než

mechanismus Michael v TKIP. Výpočet 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.

Channel	Auto
Wireless Mode	54G Only ☐ 54g Protection
Authentication Method	WPA2-Personal
WPA Encryption:	TKIP+AES
WPA Pre-Shared Key:	TKIP+AES
WEP Encryption:	None
Passphrase:	
WEP Key 1 (10 or 26 hex digits):	
WEP Key 2 (10 or 26 hex digits):	
WEP Key 3 (10 or 26 hex digits):	
WEP Key 4 (10 or 26 hex digits):	

Obr. 17.: Nastavení zabezpečení WPA2 u bezdrátového routeru ASUS WL-520gC.

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 128bitový blok. Celý vstupní text se rozdělí na 128bitové bloky a ty se postupně XORují se 128bitovým pokaždé nově generovaným výstupem AES tak dlouho, dokud nedojde k zašifrování celé původní zprávy. Nakonec se čítač vynuluje, XORuje se hodnota MIC, který se přidává na konec rámce.²⁴

Výsledkem je mnohem silnější a výkonnější šifra. Zvýšené šifrovací nároky, však při nástupu standardu 802.11i přetěžovaly procesory zařízení, založených na WEP/RC4.

²⁴ BARKEN, L. *Wi-Fi: jak zabezpečit bezdrátovou síť*. Vyd. 1. Brno: Computer Press, 2004. 174 s. ISBN 80-251-0346-3.

Z toho důvodu vyžaduje AES nový hardware a je tedy nekompatibilní, s tehdejší první generací bezdrátových zařízení.

WPA2 je v dnešní době nejlepším možným typem zabezpečení bezdrátové sítě. Prolomení ochrany je velmi obtížné. Důležité také je, že šifra AES nebyla zatím podle všech informací prolomena. Tento stav však nemůže vydržet navždy a se zvyšováním výkonu počítačů to bude stále jednodušší. V budoucnosti budou proto potřeba nové formy zabezpečení a jiné bezpečnostní standardy.

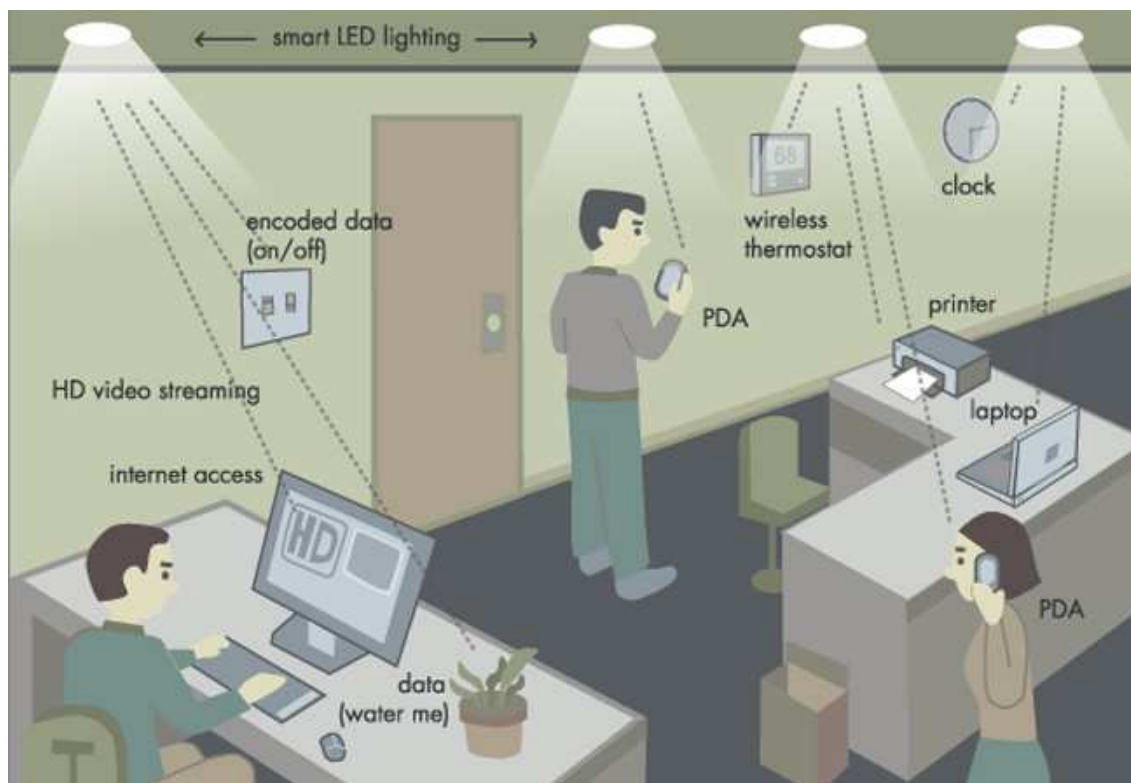
1.4 Budoucnost bezdrátových technologií

Moje prognóza budoucnosti Wi-Fi je konkrétně tato: podle mého názoru se budou uvolňovat stále další a další frekvenční pásma, čímž bude vznikat stále více nových standardů nebo se budou rapidně upravovat stávající. Čím dál větší důraz bude kladen na bezpečnost bezdrátové komunikace ale bez valného výsledku. Útočníci vždy byli a vždy budou, o krok napřed. Budou se zavádět stále složitější šifry, které budou mnohem náročnější na výpočetní výkon, než kdy předtím. Se zvyšováním výpočetního výkonu počítačů podle Moorova zákona (zákon o zvyšování výkonu počítačů – Gordon Moore v roce 1965 předpověděl, že výkon počítačů se každý rok zdvojnásobí. V dnešní době se tato tendence snižuje a platí, že výkon počítačů se zdvojnásobí přibližně za 1,5 roku) je nutnost čím dál více složitých šifer nutná. Šifry, které je nemožné v dnešní době v reálném čase prolomit, za 15 let budou neúčinné (podle Moorova zákona budou v té době 1024x výkonnější počítače, než jsou dnes). Co se týče technologie samotné, nemyslím si, že dojde v brzké době k nějaké zásadní změně. Výkon a rychlost připojení se budou stále zvyšovat, ale vše bude pracovat na stále stejných nebo velmi podobných principech. Budou se rozšiřovat oblasti používání bezdrátových technologií. Už dnes se experimentuje s nasazením bezdrátových technologií přímo uvnitř PC – to znamená, že většina drátů a kabelů uvnitř stolních počítačů, by měla být nahrazena bezdrátovým přenosem. Je otázka, zda-li potom počítače nebudou náchylnější k rušení. Posouzení nakolik tato technologie bude využitelná, nechám na Vás. Stále je to totiž spíše science fiction, než realita.

Další zajímavou technologií vyvíjí čínští vědci. Technologie má pracovat na podobném principu jako IrDA (tedy technologii přenosu dat pomocí infračerveného záření, které dosahuje maximální teoretické rychlosti až 4 Mb/s – na velmi podobné bázi funguje dálkové ovládání televizoru) „do běžných stropních LED žárovek přidali několik speciálních LED diod s modrým světlem, určených právě k přenosu dat. Tento přenos je realizován prostou modulací blikání (respektive pulsování) těchto diod a to v takovém rozsahu, které lidské oko ani nepostřehne a nesnižuje tak kvalitu osvětlení místnosti.

Touto technologií se podařilo streamovat HD videoobsah do notebooku ležícího uprostřed místnosti a podle prohlášení dosáhla špičková propustnost takto vytvořené

sítě hodnoty dvou megabitů za sekundu. Podobnou technologii podle informací magazínu Engadget, před časem testovala také Bostonská univerzita, která však používala LED diod v osvětlení k ovládání lokálních spotřebičů, s plánovaným rozšířením na přenos dat.“²⁵



Obr. 18.: Schéma sítě vytvořené pomocí technologie Smart LED Lighting.

²⁵ JANEČEK, Vladislav. *Živě.cz* [online]. 19. 5. 2010 [cit. 2010-05-30]. Čínští vědci dokáží vytvořit počítačovou síť z osvětlení v místnosti. Dostupné z WWW: <<http://www.zive.cz/bleskovky/cinsti-vedci-dokazi-vytvorit-pocitacovou-sit-z-osvetleni-v-mistnosti/sc-4-a-152369/default.aspx>>.

2 Analýza problémů

2.1 Hardware použitý v nynější síti

V této části budu popisovat – analyzovat síť. Jedná se o mou vlastní bezdrátovou síť. Potřebu bezdrátového připojení jsem pocítil přibližně před dvěma lety, kdy jsem si koupil notebook, se kterým se mohu pohybovat po celém bytě a připojení k internetu a k vlastní síti je pro mě klíčové. Samotné ethernetové připojení by tedy pro mě bylo omezením, které má více nevýhod než výhod. Jedinou výhodou je vyšší rychlost (1 Gbit/s) která je oproti 54 Mbit/s dost rapidní. Po delším užívání jsem zjistil, že to však není až tak nutné. Nevýhodami ethernetového připojení je nutnost vytvoření kabelové infrastruktury a také omezení volnosti.

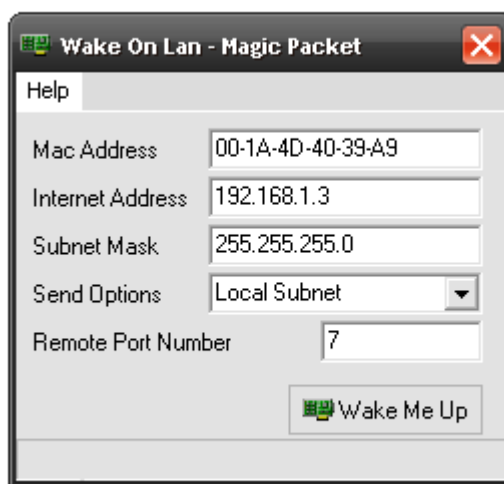
Centrem mé sítě je bezdrátový router ASUS WL-520gC. Tento router podporuje standard 802.11b/g. To znamená, že maximální teoretická rychlost je, jak už jsem napsal výše - 54 Mbit/s. Tento router nabízí velmi dobrý poměr cena/výkon, což byl jeden z největších argumentů při jeho koupi.



Obr. 19.: Bezdrátový router ASUS WL-520gC. ²⁶

²⁶ ASUSTeK computer Inc. [online]. 2009 [cit. 2010-05-09]. ASUS WL-520gC. Dostupné z WWW: <http://www.asus.cz/product.aspx?P_ID=Pq3TmwugpKCFDkV5>.

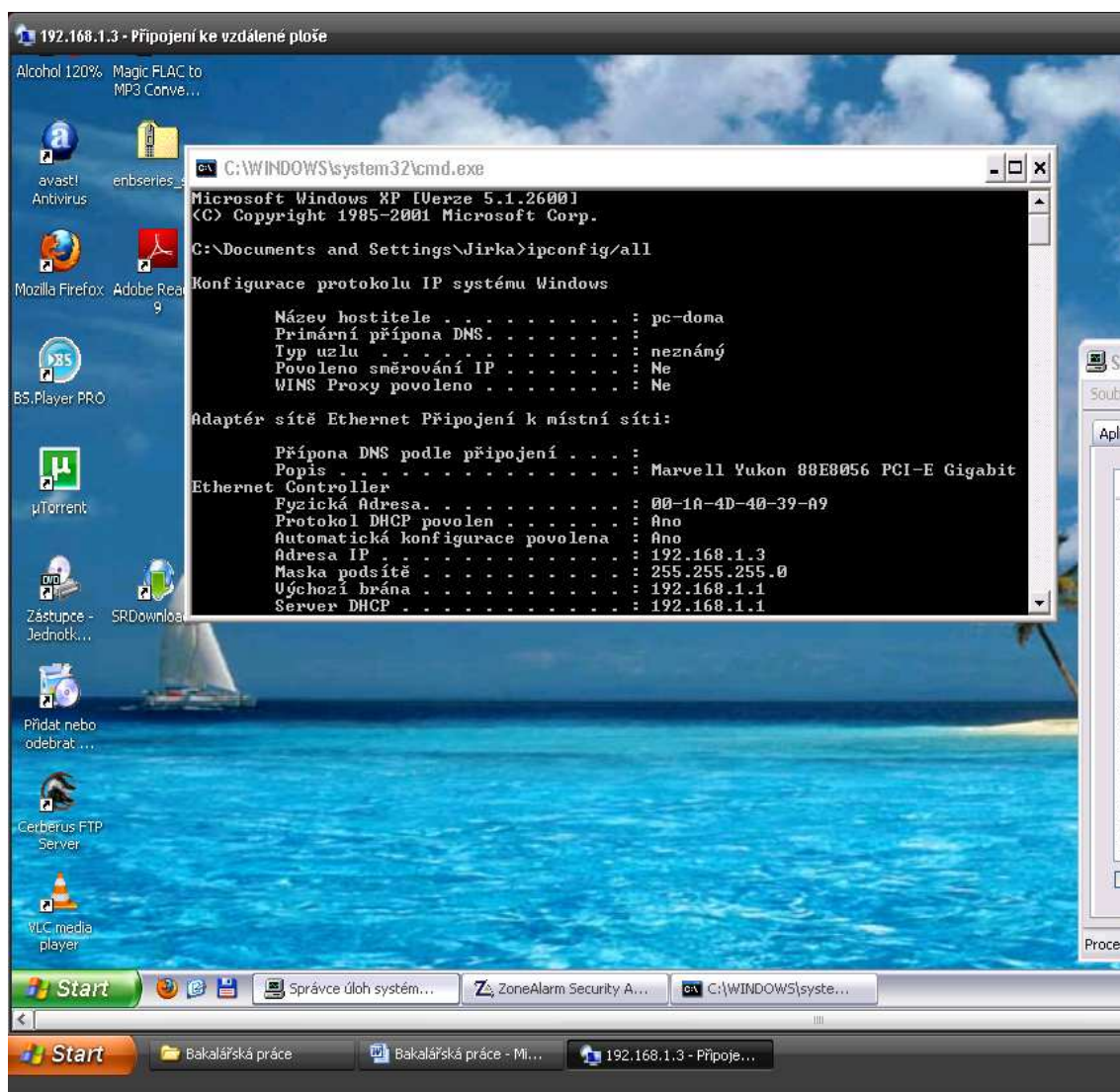
Dále je tento router vybaven čtyřmi LAN porty a jedním WAN portem, přes který je připojen k ADSL modemu a dále do sítě internet. Přes jeden z LAN portů je také připojen stolní počítač, který je hlavním úložištěm dat. Díky možnosti připojení ke vzdálené ploše, lze tento počítač ovládat na dálku a díky možnosti Wake on LAN, lze pomocí jiného počítače tento počítač zapnout na dálku. Tato funkce je možná díky podpoře základní desky a speciálního programu na počítači, kterým chceme vzdálený přístroj zapnout. Tento program vyšle tzv. Magický paket, který má podobu šesti stejných bajtů, hexadecimálně zapsaných jako FF:FF:FF:FF:FF:FF, které jsou následovány šestnáctkrát opakující se MAC adresou.



Obr. 20: Wake On Lan – Magic Packet – utilita na zasílání „Magického Paketu“.

Dalším zařízením připojeným do mé sítě je notebook, který je připojen přes Wi-Fi standard 802.11g. Přes tento notebook je ovládán i stolní počítač, pomocí programu Vzdálená Plocha. Tento program nabízí kompletní možnost ovládání vzdáleného počítače. Je součástí systému Windows a stejně jako u Wake on LAN je nutné povolit možnost připojení na vzdáleném počítači (což se ve Windows XP SP3 dělá v nabídce vlastností: Tento počítač => záložka vzdálený přístup => a zatržení Povolit připojení vzdálených uživatelů k tomuto počítači). Poté stačí spustit program v nabídce Start (Windows XP SP3 => Všechny programy => Příslušenství => Připojení ke vzdálené ploše), v tomto programu pak již jen stačí v možnostech připojení vyplnit IP adresu

počítače a jméno uživatele. Při připojení je pak nutné zadat heslo administrátora. Po připojení program nabízí úplné ovládání vzdáleného počítače pomocí okna, ve kterém je plocha vzdáleného počítače. Jediné činnosti, které jsou při připojení pomocí vzdálené plochy částečně omezeny jsou: přehrávání videa a hraní náročnějších her, přímo v okně vzdálené plochy (je to z důvodu vyššího datového toku který buď program nebo připojení nemusí zvládat). Pokud je použití vzdálené plochy omezeno jen na použití v rámci LAN, je dobré v možnostech vzdálené plochy na záložce Výkon vybrat položku „sít LAN (10 Mbps nebo vyšší)“, díky této možnosti bude program využívat připojení opravdu naplno a většina datově náročnějších přenosů (jako je třeba zobrazování tapety plochy atd.) bude povolena.



Obr. 21: Ukázka připojení ke vzdálené ploše.

Připojení ke vzdálené ploše stejně jako Wake on LAN se neomezuje jen na lokální síť. Je možné se připojit přes internet, z nějakého opravdu vzdáleného počítače. V tomto případě je však nutné znát veřejnou IP adresu dané sítě a také v rámci routeru nastavit přesměrování portů. V tomto případě je to port číslo 3389 (u Wake on LAN je to port číslo 7). Toto nastavení zajistí aby bylo dané připojení přesměrováno na příslušný počítač v síti.

NAT Setting - Virtual Server

To make services, like WWW, FTP, provided by a server in your local network accessible for outside users, you should specify a local IP address to the server. Then, add the IP address and network protocol type, port number, and name of the service in the following list. Based on the list, the gateway will forward service request from outside users to the corresponding local server.

Enable Virtual Server? ☒ Yes ☐ No

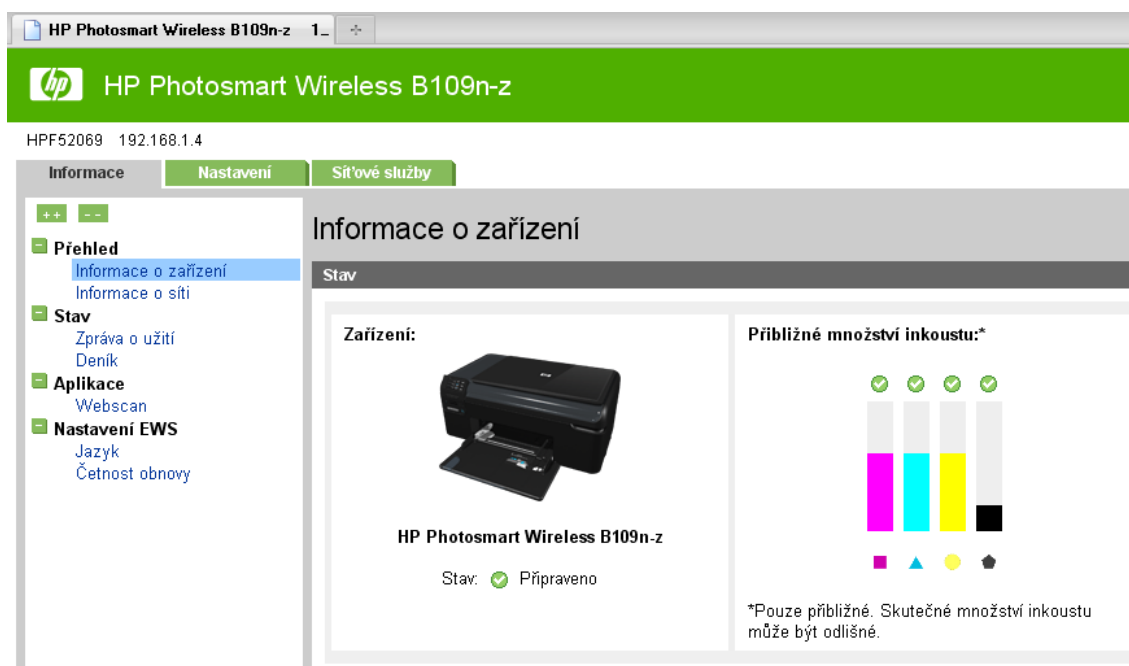
Virtual Server List

Well-Known Applications:		User Defined ▼		
Port Range	Local IP	Local Port	Protocol	Description
			TCP ▼	
23050	192.168.1.2	23050	TCP	uTorrent notebook
21	192.168.1.3	21	TCP	FTP Server
3389	192.168.1.3	3389	TCP	Vzdálená plocha
62726	192.168.1.3	62726	TCP	uTorrent desktop

Obr. 22.: Nastavení přesměrování portů u bezdrátového routeru ASUS WL-520gC.

Posledním zařízením připojeným do mé sítě je tiskárna HP Photosmart Wireless B109n-z, která nabízí možnost připojení právě pomocí Wi-Fi. Tímto způsobem odpadají komplikace s nutností tisknutí přes stolní počítač, v případě tisknutí z notebooku přes Wi-Fi. Nyní v případě tisknutí z notebooku nemusí být stolní počítač vůbec zapnutý. Veškerá komunikace se tak odehrává pomocí Wi-Fi. V případě nutnosti, lze využít i přes webové rozhraní tiskárny (to například v případě, že uživatel nemá nainstalovány ovladače pro tiskárnu na počítači). Na tomto rozhraní je i většina důležitých informací ohledně tiskárny a dokonce možnost skenování přes toto rozhraní.

Je zde i většina nastavení týkající se připojení k síti. Tiskárna má IP adresu 192.168.1.4 a při zadání této adresy do okna prohlížeče, se uživatel dostane na toto webové rozhraní.



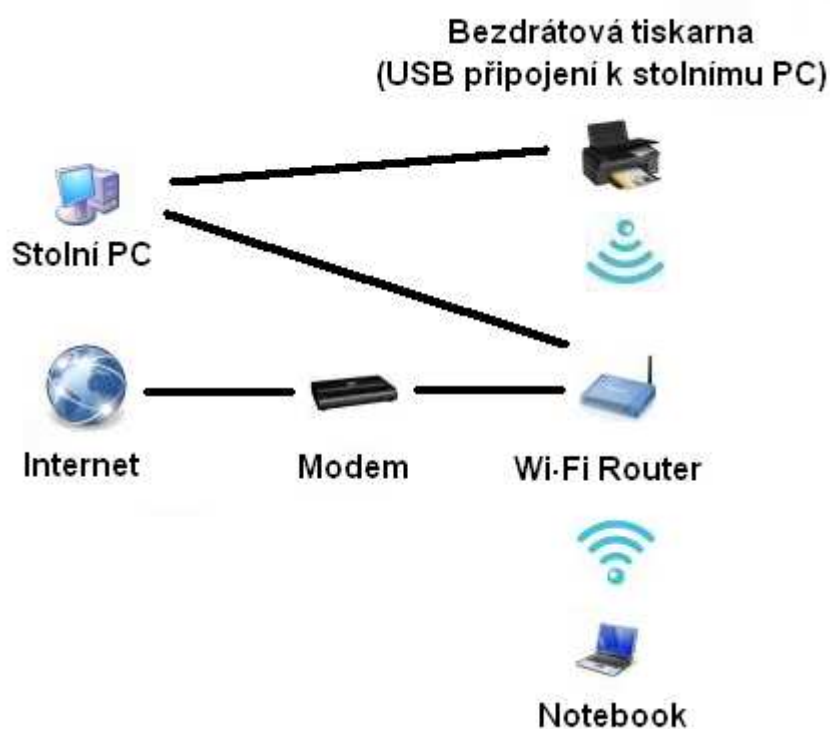
Obr. 23.: Webové rozhraní tiskárny HP Photosmart Wireless B109n-z.

Při skenování dokumentu lze přímo na tiskárně vybrat, do kterého z počítačů v síti se data přenesou a po potvrzení, se v případě skenování spustí příslušná aplikace pro úpravu neskenovaného dokumentu.

Název zařízení	IP adresa zařízení	Sít'. název zařízení	Popis
ASUS WL-520gC	192.168.1.1		Bezdrátový router
Dell Vostro 1500	192.168.1.2	NOTEBOOK	Notebook
Stolní PC	192.168.1.3	PC-DOMA	Domácí PC
HP Photosmart Wireless B109n-z	192.168.1.4		Bezdrátová tiskárna

Tabulka 1.: Přehled připojených zařízení do sítě (k routeru je ještě připojen modem Motorola).

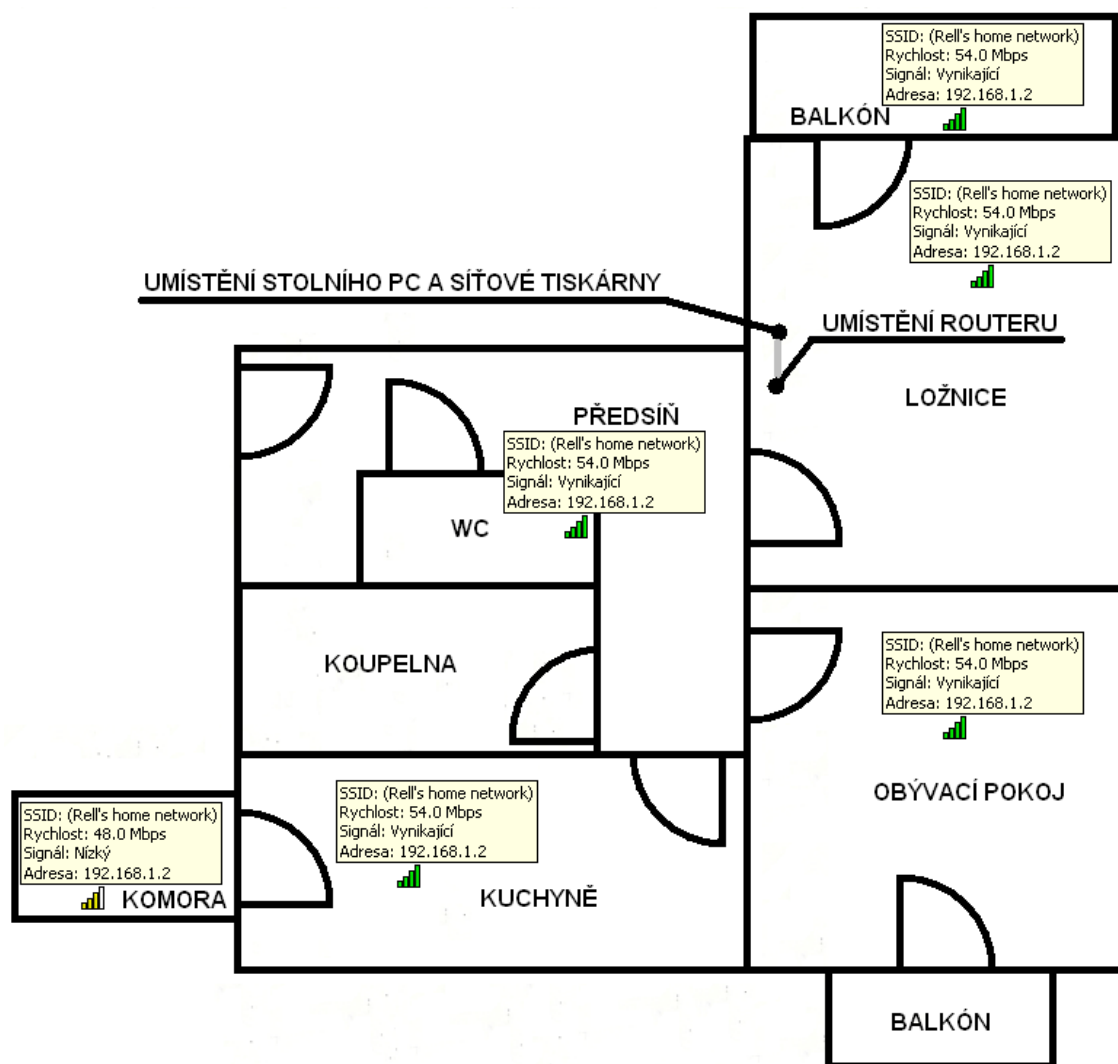
Důležitou skutečností je to, že všechny zařízení v síti mají pevně nastavenou IP adresu. V případě dynamické změny IP adres v síti, by docházelo ke změnám IP adres u všech zařízení a bylo by velmi problematické připojovat se například pomocí vzdálené plochy (při každém pokusu o připojení, by bylo nutné napřed zjistit aktuální IP adresu zařízení a až poté se připojit).



Obr. 24.: Schéma sítě.

Co týče stolního počítače ten hraje roli serveru. Většina dat je uložena v něm a v notebooku je jen minimum nezbytně nutných dat a také zálohy důležitých dat. Je to hlavně z důvodu kapacity obou zařízení. Notebook má pouze 320 GB disk (rozdělený na dva logické oddíly 30 GB systémový a druhý 268 GB pro dokumenty atd.), ale ve stolním PC jsou dva 1TB disky, jeden 640 GB disk, jeden 320 GB disk a přenosný 2,5 palcový 80GB disk v rámečku. 320 GB disk je ještě rozdělen na dva logické oddíly, jeden o velikosti 40 GB, který je systémový, a druhý o velikosti 258 GB. Všechny disky, kromě systémových, jsou nasdíleny a lze se na ně kdykoliv (samozřejmě když je zařízení zapnuto) připojit a pracovat s daty, které jsou na nich uloženy.

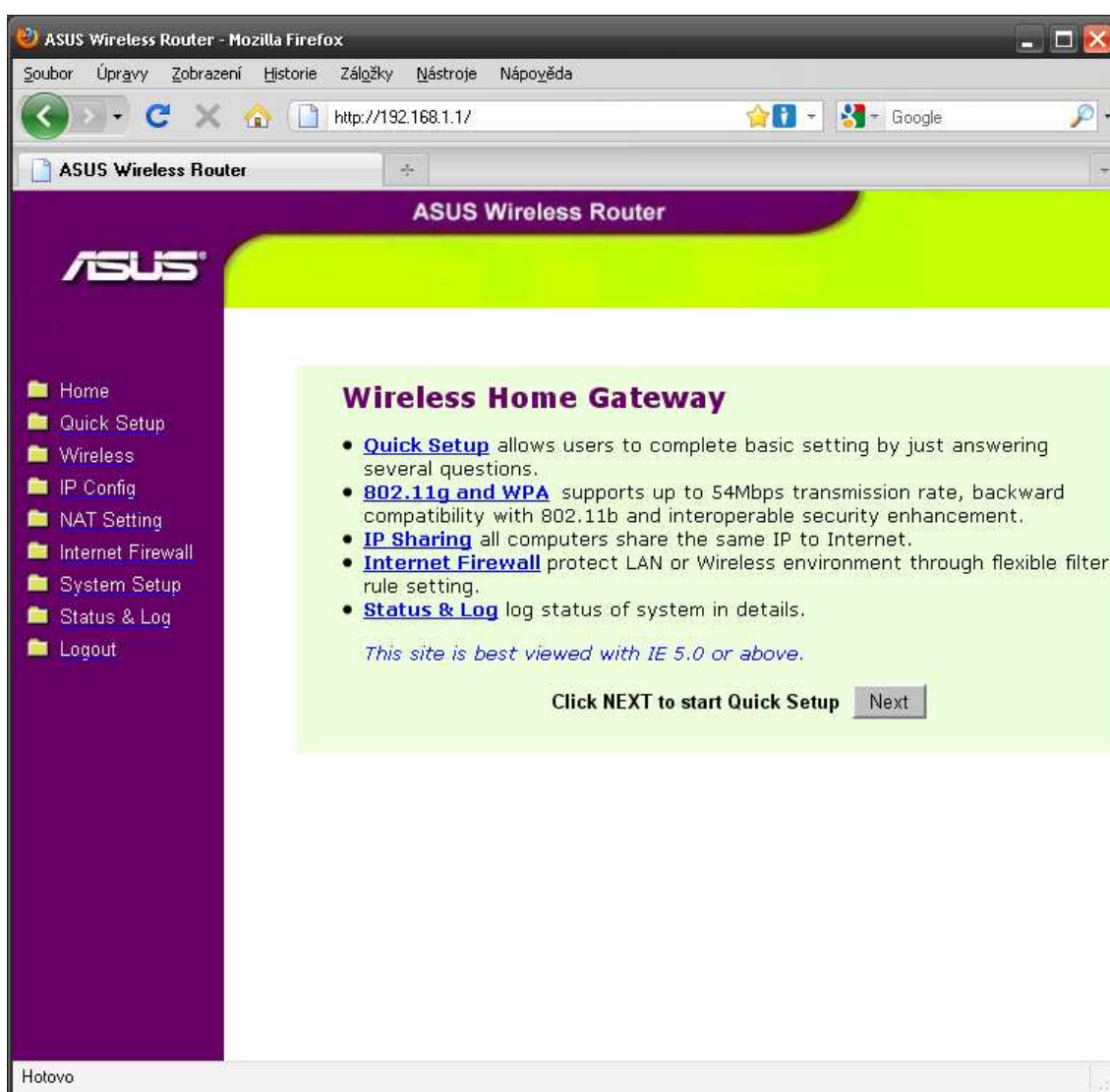
Signál bezdrátové sítě je po celém bytě velmi dobrý. V ložnici a obývacím pokoji je signál výborný a reálná přenosová rychlost dosahuje 25 až 30 Mbit/s (teoretická je dokonce plná, tedy až 54 Mbit/s). Tato situace je způsobena tím, že přímo v ložnici je umístěn bezdrátový router a obývací pokoj je od ložnice oddělen jen sádkartonovou příčkou, která ruší signál bezdrátové sítě jen minimálně.



Obr. 25.: Půdorys bytu s vyznačeným umístěním routeru, stolního PC a síťové tiskárny, a silou signálu.

Dokonce i na balkóně, v předsíni a v kuchyni je signál plný, i když jsou od ložnice odděleny širšími zdmi, které mohou signál rušit více. Jediná věc, která indikuje rušení, je mírný pokles reálné přenosové rychlosti, která se pohybuje okolo 20 Mbit/s (teoretická se stále zobrazuje jako plná – 54 Mbit/s).

Nejhorší signál jev místnosti za kuchyní - v komoře, kde se reálná přenosová rychlost pohybuje okolo 10-12 Mbit/s (teoretická se snížila na 48 Mbit/s). Tento fakt, však nijak neomezuje možnosti připojení, protože v komoře není uložen žádný hardware, který by vyžadoval bezdrátové připojení k síti. Celkově hodnotím kvalitu a výkon připojení velmi pozitivně na veškeré činnosti, jako je například přehrávání videa ze síťového disku (zatím však jsem nezkoušel přehrávání videa ve velmi vysokém HDTV rozlišení, jako je například 1920x1080 px. S tímto rozlišením lze očekávat problémy, kvůli velmi vysokému datovému toku). Co se týče videa v normálním rozlišení, je přehrávání plynulé a neobjevují se žádné problémy.



Obr. 26.: Webové rozhraní bezdrátového routeru ASUS WL-520gC.

Router samotný nabízí, stejně jako bezdrátová tiskárna webové rozhraní, které slouží k nastavení všech parametrů sítě – od použitého zabezpečení sítě, přes výběr jména sítě, až po pokročilejší nastavení, jako je přeměrování portů a tak dále. Toto webové rozhraní je přístupné po zadání IP adresy routeru do adresního řádku prohlížeče (viz obrázek 25).

2.2 Zabezpečení nynější bezdrátové sítě

Síť samotná je zabezpečena pomocí WPA2 a navíc použitím filtrování MAC adres. Toto zabezpečení hodnotím jako dostatečné a myslím si, že v mém případě nehrozí nabourání do sítě. Podle mého názoru není nutné používat další zabezpečení, jako je třeba skrytí SSID.

WPA2 samotné, by také podle mého názoru bohatě stačilo, ale použití filtrování MAC adres nepřináší žádné nevýhody (snad kromě nutnosti dodatečného přidání MAC adresy, při připojení dalšího zařízení do sítě) a proto mám za to, že další bezpečnostní opatření jen přispěje k bezpečnosti.

Dalším důležitým bezpečnostním opatřením je zabezpečení webového rozhraní samotného Wi-Fi routeru. Na tuto skutečnost dost uživatelů zapomíná, přestože následky útoku na tuto bezpečnostní slabinu by mohly být fatální. Samotný router je zabezpečen přístupovým jménem a heslem. Toto bezpečnostní opatření je nutné během prvního spuštění bezdrátové sítě nastavit. Pokud by uživatel takto neučinil, útočník se může po zadání IP adresy sítě dostat do nastavení routeru a změnit veškeré nastavení sítě, od zabezpečení přes jméno sítě, až po samotné heslo k routeru. Čímž majiteli znemožní přístup do routeru. Většina bezdrátových routerů sice má tlačítko na vynulování nastavení, ale i tak by tento útok mohl pro uživatele znamenat velké komplikace, nemluvě o tom, že útočník si například tímto způsobem může otevřít zadní vrátka do celého systému a ve chvíli, kdy se dostane do dosahu bezdrátové sítě, má kompletní přístup ke všem datům, které má uživatel sítě nasdíleny.

Na internetu je mnoho případů nezabezpečených routerů, webových kamer, síťových tiskáren a dalších zařízení, které uživatelé dostatečně nezabezpečili a tak se mohou stát terčem útoku. V případě routeru má útočník práci velmi usnadněnou, protože může po chvíli začít ovládat celý systém.

Podobný případ je zabezpečení síťové tiskárny. Ta sice nepředstavuje takový problém, co se týče nebezpečnosti, nebo největšího možného rozsahu spáchaných škod. Pokud by se útočník chtěl dostat do nastavení tiskárny, musel by před tím překonat samotné WPA2 zabezpečení, což je velmi nepravděpodobné. Přesto je však důležité

nepodceňovat ani toto zabezpečení a při prvním použití, okamžitě nastavit přihlašovací jméno a heslo.

let's warchalk..!	
KEY	SYMBOL
OPEN NODE	ssid  bandwidth
CLOSED NODE	ssid 
WEP NODE	ssid access contact  bandwidth
blackbeltjones.com/warchalking	

Obr. 27.: Warchalking symboly.²⁷

Samotnou skutečnost, že velký počet uživatelů nemá vůbec zabezpečenou bezdrátovou síť považuji za velmi alarmující. Samotní uživatelé si vůbec neuvědomují

²⁷ Pooh.cz [online]. 2005 [cit. 2010-05-30]. Warchalking a WiFi sítě vůbec. Dostupné z WWW: <<http://www.pooh.cz/clanky/warchalking/warchalking.asp>>.

v jakém riziku se nacházejí oni samotní i jejich data. Trend má sice sestupnou tendenci a většina uživatelů si začíná postupně uvědomovat hrozící nebezpečí a použije některou formu zabezpečení. Podle statistik je dokonce jen v Praze 16%²⁸ všech bezdrátových sítí nezabezpečených, toto číslo je rozhodně lepší než v minulých letech, přesto by bylo z hlediska bezpečnosti mnohem lepší, kdyby bylo zabezpečeno všech 100% sítí.

Ve světě dokonce existuje takzvaný Warchalking, což je vlastně usnadnění pro uživatele, kteří se chtějí připojit do cizí sítě (většinou bez špatného úmyslu – chtějí se jen připojit na internet). Pro tyto uživatele byly vytvořeny tři značky, které je informují o stavu zabezpečení sítí v dosahu. Většinou tyto značky bývají nakresleny někde na zdi, kde je neznalý uživatel považuje za další výplod nějakého sprejera. Pro zasvěceného člověka, však poskytuje informaci, zda je síť v dosahu úplně otevřená (nad obrázkem je i její SSID pro snadnější nalezení), chráněná skrytím SSID, nebo WEPem (viz obrázek 26).

²⁸ *ITBiz.cz* [online]. 8.11.2009 [cit. 2010-05-30]. V Praze je zabezpečených 84 % WiFi sítí. Dostupné z WWW: <<http://www.itbiz.cz/praha-zabezpeceni-wifi-pripojeni>>

2.3 Analýza problémů

Samotná síť popsaná v předchozích dvou částech této kapitoly funguje velmi dobře, ale již delší dobu uvažuji o jejím rozšíření, popřípadě přestavbě a také o přidání dalších funkcí, jako je třeba FTP server atd.

Prvním problémem je skutečnost, že v obývacím pokoji je televize která je připojena na DVD přehrávač, ale není nijak připojena do sítě (DVD přehrávač je sice vybaven pevným diskem, ale neobsahuje žádné síťové rozhraní). Na této televizi by se daly přehrávat multimédia mnohem lépe, než na stolním PC, popřípadě notebooku.

Druhý problém úzce souvisí s prvním. Ve chvíli kdy bude potřeba na televizi přehrávat filmy ve vysokém rozlišení například 1080p, které televize podporuje, rychlost připojení k bezdrátové síti může být při vysokém datovém toku filmu nedostačující. Tento film ve vysokém rozlišení, pak nebude možné streamovat ze stolního PC - serveru.

Třetím problémem je umístění stolního PC – serveru celé sítě v ložnici. Tento počítač, který je zapnutý prakticky pořád, může rušit obyvatele ložnice, například při spánku a to i přesto, že jsem se při jeho stavbě snažil použít co možná nejtišší komponenty.

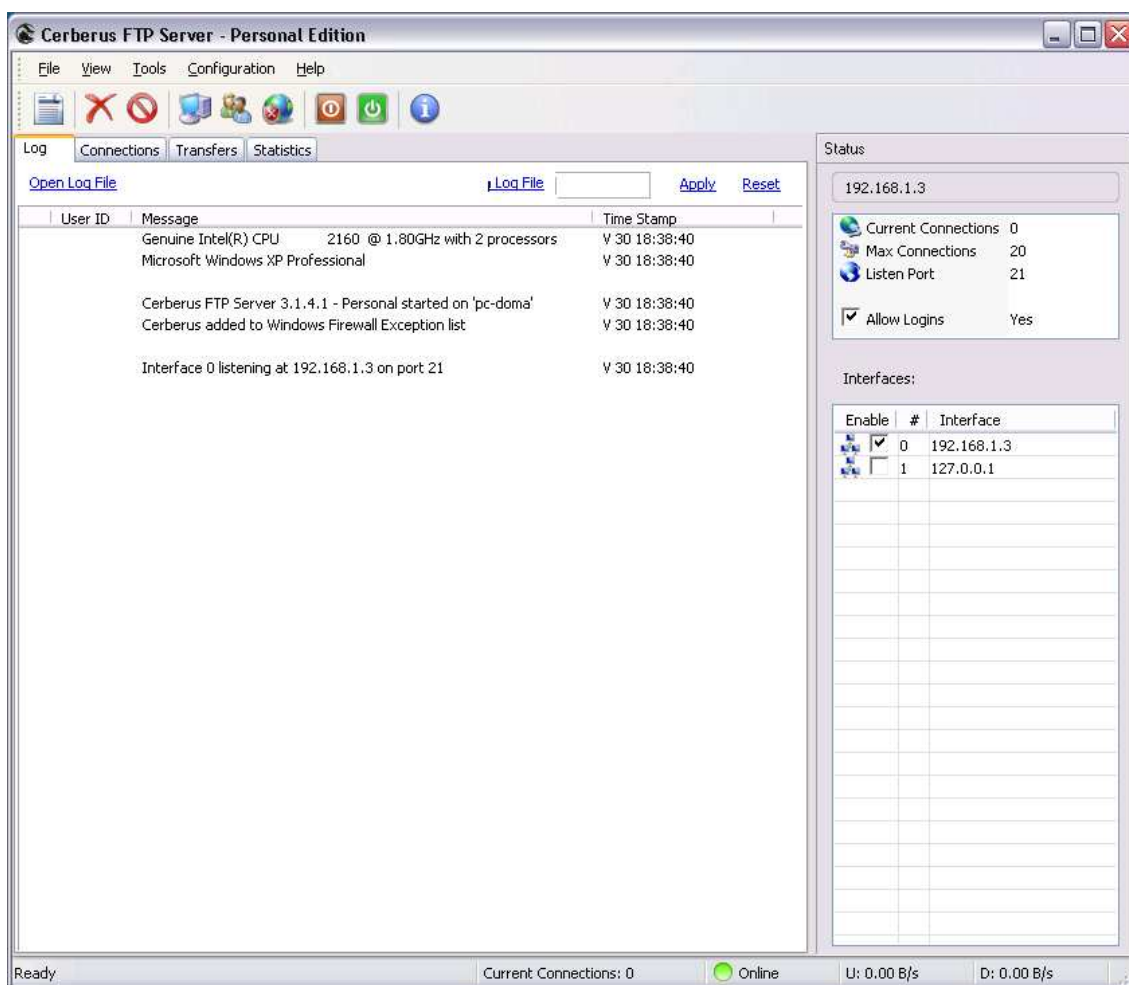
Posledním úkolem je zjistit možnosti připojení do bezdrátové sítě pomocí telefonu nebo smarphonu, vybaveného pro připojení do bezdrátové sítě.

3 Vlastní návrhy řešení

3.1 FTP server

FTP server je velmi užitečná věc a v případě, že stolní PC je stále zapnutý, přístup k tomuto serveru nic neomezuje. FTP server může být využíván mnoha způsoby. Například pokud existují nějaká data, která je nutné nasdílet i s ostatními lidmi, není jednodušší způsob, jak toto provést než využít FTP server.

Na internetu existuje mnoho programů, které lze k vytvoření FTP serveru využít. Jeden z nejlepších Cerberus FTP Server je dokonce pro nekomerční použití zdarma.



Obr. 28: Okno programu Cerberus FTP Server.

Jak již jsem nastínil v předchozí kapitole, středobodem celé sítě je bezdrátový router ASUS WL-520gC. Z této skutečnosti vyplývá mírná komplikace oproti situaci, kdyby jako FTP server byl počítač, připojený přímo do internetu. Je nutné nastavit

správně přesměrování portů, aby se data odesílaná routerem, šla od správného počítače v síti.

Pro FTP komunikaci jsou využívány porty 20 popřípadě 21. Je to nepsané pravidlo a není nutné jej dodržovat, ale ve většině případů to bývá právě takto. U bezdrátového routeru ASUS WL-520gC je toto nastavení velice jednoduché (viz. obrázek 21). Dále je nutné nastavit stejný port v programu Cerberus FTP Server. Také je důležité nastavit, která složka bude sdílena přes FTP a jaká budou mít připojení uživatelé práva (jestli mohou data uložená ve sdílené složce i upravovat a třeba i mazat nebo jen si je zkopírovat). Sdílených složek může být velmi mnoho a také počet profilů je prakticky neomezený. Pak už stačí jen nastavit heslo a společně s jménem relace, IP adresou a uživatelským jménem jej zaslat všem, kterým je nutné daná data nasdílet.

Uživatelé si pak pomocí některého z programů (například pomocí Total Commanderu) data jednoduše stáhnou. V případě využití Total Commanderu, však pozor na ukládání relací. Pokud se nějaká neoprávněná osoba bude snažit dostat na daný FTP server, ve většině případů může právě využít uložených hesel v TC, která nejsou nijak zabezpečena.

3.2 Připojení TV v obývacím pokoji do sítě

Jak jsem již napsal v předešlé kapitole, bylo by velmi dobré připojit TV v obývacím pokoji do sítě pomocí nějakého síťového přehrávače. V tomto případě lze uvažovat o dvou koncepcích. První z nich je využít ethernetového připojení z routeru přímo do síťového přehrávače. Toto řešení jsem zavrhl, protože je úplně zbytečné ve chvíli, kdy je k dispozici možnost bezdrátového připojení.

Druhou možností je využít některého ze síťových přehrávačů, které nabízí možnost bezdrátového připojení, buď již v základu nebo je možné rozšířit je o bezdrátovou kartu - například do slotu miniPCI.

Je nutné brát v úvahu výkon přehrávače, protože přehrávání formátu H.264 v rozlišení 1080p je velmi náročné na výpočetní výkon a nezvládne jej každý přehrávač. Dále je nutné, aby přehrávač podporoval české titulky, což je v dnešní době nutností.



Obr. 29: Přehrávač Popcorn Hour C-200 Blu-ray ready.²⁹

Jako nejlepší (i když trochu dražší) volba se mi jeví přehrávač Popcorn Hour C-200 Blu-ray ready. Tento přehrávač v sobě sice nemá zabudovanou bezdrátovou kartu, ale disponuje miniPCI slotem pro přidání této karty a samotné rozšíření není nic obtížného.

²⁹ ALFA COMPUTER a.s. [online]. 2010 [cit. 2010-05-30]. Popcorn Hour C-200 Blu-ray ready. Dostupné z WWW: <<http://www.alfacomp.cz/php/product.php?eid=10514008V000000UTE>>.

Další důležitou vlastností tohoto přehrávače je přítomnost slotu pro interní Blu-ray mechaniku, která se do přehrávače taky velmi jednoduše přidá. Tato vlastnost není nutností, protože ve chvíli, kdy bude tento přehrávač využíván jako síťový, je výhodnější Blu-ray mechaniku namontovat do počítače, protože Blu-ray média nemusí být využívána jen pro filmy, ale třeba jako zálohovací prostředky. Samotný přehrávač je také velmi výkonný a přehrávání nejnáročnějších formátů zvládá velmi dobře.



Obr. 30: Bezdrátová miniPCI karta MikroTik RouterBOARD R52N miniPCI.³⁰

Další důležitou komponentou je bezdrátová miniPCI karta, která je nutná abychom mohli přehrávač připojit do bezdrátové sítě. Měli bychom počítat s tím, že budeme bezdrátovou síť vylepšovat, proto je nutné vybrat bezdrátovou miniPCI kartu,

³⁰ ALFA COMPUTER a.s. [online]. 2010 [cit. 2010-05-30]. MikroTik RouterBOARD R52N miniPCI. Dostupné z WWW: <<http://www.alfacomp.cz/php/image.php?eid=10F140WFC&bigimg=40491av.jpg>>.

s podporou standardu 802.11n. Takovou kartou je například MikroTik RouterBOARD R52N miniPCI, která podporuje všechny standardy – tedy a/b/g/n. Samotná instalace přehrávače do sítě by neměla být problém. V síti bude podporovat veškerá zabezpečení. Je také důležité zvážit, jestli je nutné vybavovat přehrávač pevným diskem. Pokud bude fungovat jako síťový přehrávač, není to podle mě nutné – veškerý obsah se bude stramovat z lokální sítě.

3.3 Zvýšení přenosové rychlosti sítě pro přehrávání 1080p filmů

Zvýšení rychlosti sítě je nutné v případě, že si uživatelé budou chtít přehrát na síťovém přehrávači filmy, v rozlišení 1080p – tedy 1920x1080 pixelů. Datový tok se stále zvyšuje, je tedy dost pravděpodobné, že rychlost připojení k bezdrátové síti přestane být v budoucnu dostačující.

Proto je nutné zvýšit přenosovou rychlost sítě, čehož lze docílit jen přechodem na standard 802.11n, který nabízí teoretickou rychlost 300 Mbit/s a v budoucnosti lze očekávat i více.



Obr. 31: Bezdrátový router ASUS RT-N16.³¹

³¹ASUSTeK computer Inc. [online]. 2009 [cit. 2010-05-09]. ASUS WL-520gC. Dostupné z WWW: <http://www.asus.com/product.aspx?P_ID=WAA6AQFncrceRBEo>.

Pro zvýšení přenosové rychlosti sítě tedy bude nutné vyměnit centrální prvek sítě, kterým je router ASUS WL-520gC, který podporuje jen standardy 802.11b/g. Tento router bude muset být vyměněn za zařízení podporující standard 802.11n. Takovým zařízením může být třeba router ASUS RT-N16, který podporuje všechny bezpečnostní standardy jako je například WEP, WPA, WPA2.

Problém by mohl nastat v případě, že se i nadále bude v síti využívat zařízení podporující maximálně standard 802.11g. Tato skutečnost by mohla velmi snižovat výkon celé sítě, založené na standardu 802.11n.

V síti by po připojení síťového přehrávače, figurovaly dvě zařízení podporující maximálně standard 802.11g – notebook a síťová tiskárna. Co se týče síťové tiskárny je řešení velmi jednoduché. Router ASUS RT-N16 totiž nabízí podporu print serveru, což znamená, že síťová tiskárna by mohla být přes rozhraní USB 2.0 připojena přímo, do bezdrátového routeru. Co se týče notebooku, naskýtá se řešení v podobě využití karty do ExpressCard slotu, rozšiřující konektivitu notebooku. Takovou kartou je například D-link Xtreme N Notebook ExpressCard, která podporuje standard 802.11n.



Obr. 32: Karta do ExpressCard slotu D-link Xtreme N Notebook ExpressCard.³²

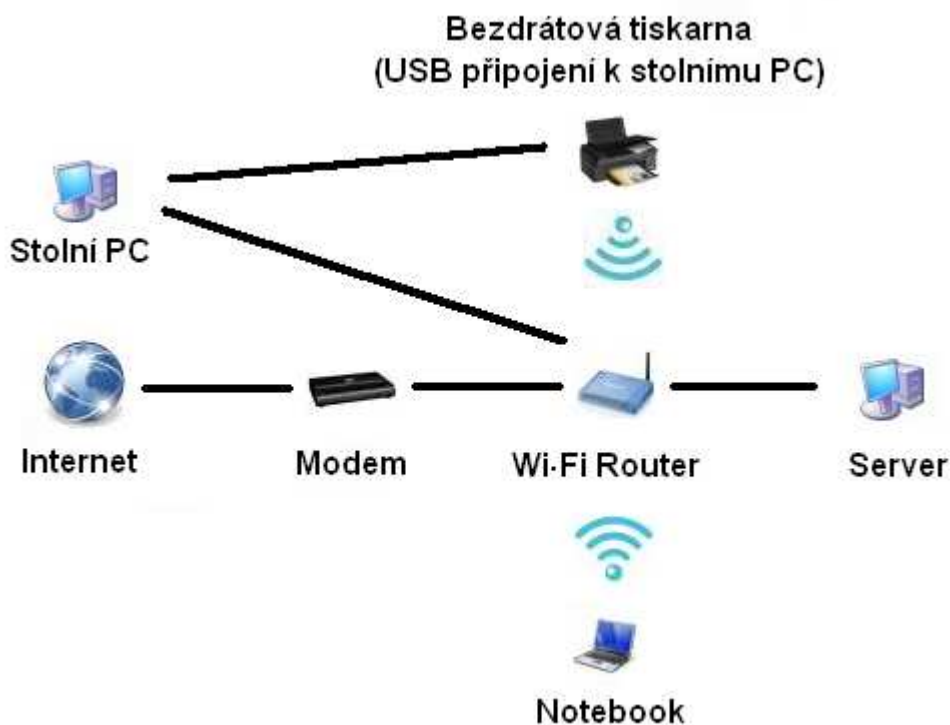
³² D-Link - Home & Home Office [online]. 2010 [cit. 2010-05-30]. DWA-643 Xtreme N Notebook ExpressCard. Dostupné z WWW: <<http://www.dlink.com/products/?pid=550>>.

3.4 Umístění serveru

Umístění serveru v ložnici je problém, protože i přes důraz na jeho co nejtišší chod, může rušit obyvatele ložnice při spánku. S přesunem tohoto počítače na nějaké jiné místo, však vyvstávají další problémy. Jeden z nejhlavnějších je ten, že server zároveň slouží jako hlavní domácí počítač. Při jeho přesunu na nějaké jiné místo, by tato funkce již nebyla možná.

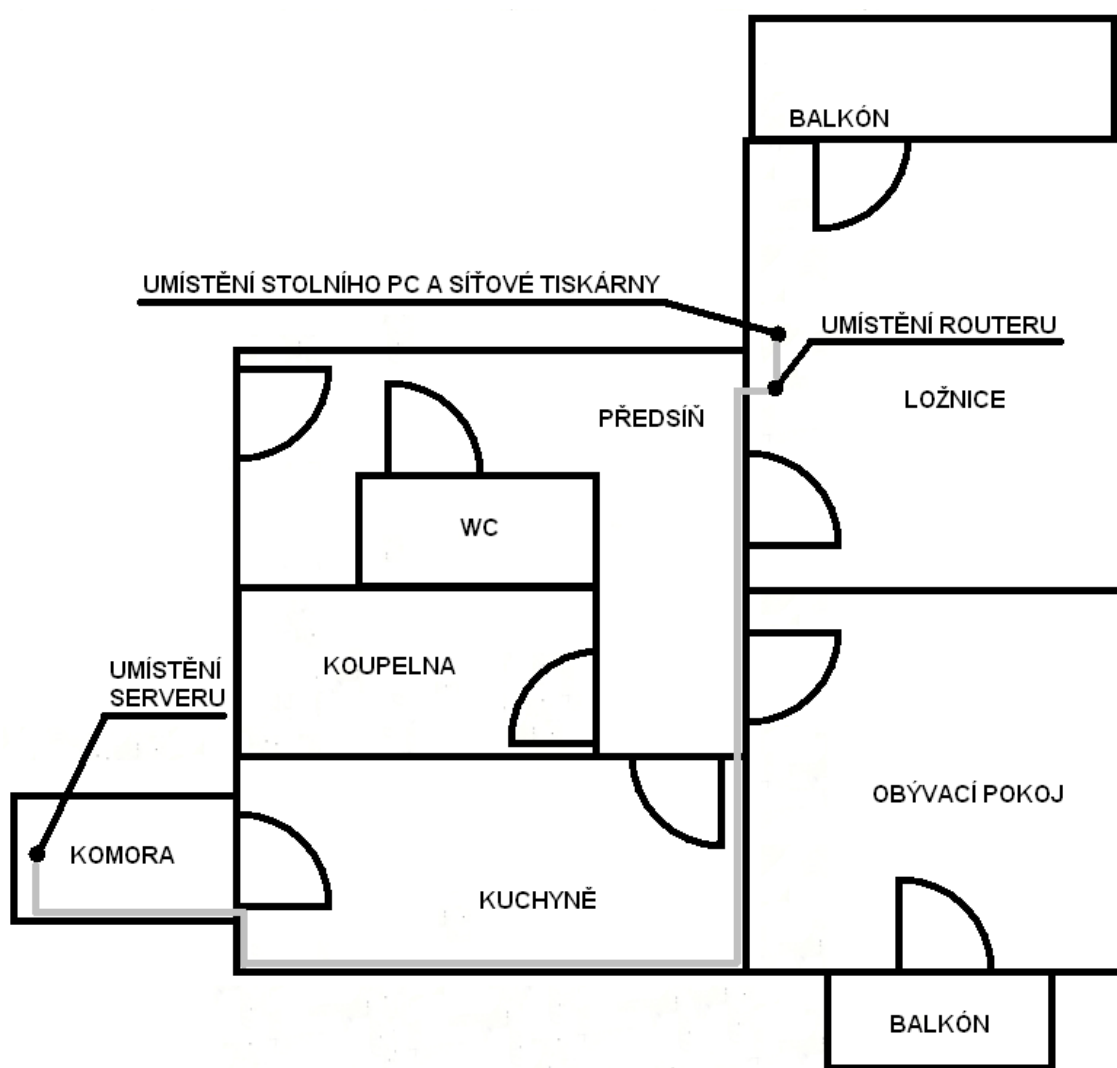
Řešením mohl být přesun s tím, že na jeho místo přijde nějaký jiný, třeba i levnější počítač, který by sloužil spíše jen jako terminál, s jehož pomocí by se uživatelé dostávali k datům uloženým na serveru.

Pokud by se daná situace řešila tímto způsobem, byla by nutná změna infrastruktury celé sítě. Jako nejlepší se jeví přesun serveru do místnosti za kuchyní, která slouží jako komora. V této místnosti se lidé běžně nepohybují a má i další výhody. Je vybavena odvětráváním, což umožní kompenzovat výkyvy teplot a dokonce zabránit přehřívání.



Obr. 33.: Schéma sítě po zapojení serveru.

Samotný počítač by nemusel být vybaven ani monitorem, klávesnicí nebo myší. Tyto periferie by se k počítači připojily jen v případě nějakých výraznějších úprav systému (formátování systémového disku, instalace operačního systému, instalace ovladačů síťové karty atd.). Při každodenních změnách by stačilo používání připojení ke vzdálené ploše. Toto řešení by výrazně zlevnilo pořizovací náklady nového počítače, protože kromě samotného PC by se již nic jiného nemuselo kupovat kupovat. Lze použít všechny komponenty, které jsou připojeny k stávajícímu stolnímu PC - serveru nyní.



Obr. 34.: Půdorys bytu s vyznačeným umístěním routeru, PC, síťové tiskárny, a serveru.

Při koupi nového PC je nutné zvážit, na co bude používán. Pokud bude sloužit opravdu jen jako terminál, není nutné do něj investovat vysoké peněžní částky. Stačí

vybrat nějaké průměrně výkonné kancelářské PC. Opačný případ nastane, pokud některý z uživatelů bude chtít na stolním PC například hrát náročné hry, nebo pracovat v nějakém programu, s vyššími nároky na výkon. V tom případě, se vyplatí investovat do PC větší obnos.

V prvním případě je ideální například počítač Compaq 500B, který lze v dnešní době pořídit za cenu okolo sedmi a půl tisíce korun (specifikace jsou v tabulce číslo 2). Tento počítač, by plně odpovídal požadavkům uživatelů v případě, že uvažujeme o prvním případě. Jediná věc, která by se na PC mohla změnit je síťová karta. Je možné, že bude nutné přenášet mezi serverem a stolním počítačem velké datové objemy. Proto by bylo vhodnější, stolní počítač vybavit síťovou kartou, podporující ethernetové přenosy rychlostí 1 Gbit/s. Například kartou TP-LINK TG-3468, která se dá sehnat za cenu 200 korun.

Procesor	Intel Pentium Dual Core E5400 2.7GHz
Operační paměť	2GB DDR3
Grafická karta	Integrovaná, Intel Graphics Media Accelerator X4500 HD
Pevný disk	320 GB SATA II, 7200 otáček za minutu
Síťová karta	10/100 Mbit/s

Tabulka č. 2.: Sestava PC Compaq 500B.³³

V druhém případě doporučuji výkonnější počítač složit – tedy koupit jednotlivé komponenty a složit je dohromady. Složení PC je nejen ve většině případů levnější, než koupě sestavy, uživatel navíc není omezen zárukou a může PC kdykoliv upgradovat, a také složené PC může lépe splnit konkrétní požadavky, toho kterého uživatele.

Server bude připojen ethernetem k routeru rychlostí 1Gbit/s. Toto řešení jsem vybral ze dvou důvodů. Prvním je skutečnost, že kvalita signálu v místnosti za kuchyní

³³ ALFA COMPUTER a.s. [online]. 2010 [cit. 2010-05-31]. Compaq 500B. Dostupné z WWW: <
<http://www.alfacomp.cz/php/product.php?eid=10514008R000000X4Z>>.

je nižší, než v celém bytě – to by mohlo snižovat rychlost bezdrátového připojení a omezovat tak možnosti serveru. Druhým důvodem je to, že síťová komunikace mezi serverem a ostatními prvky sítě bude probíhat prakticky neustále a mohla by tak přetěžovat bezdrátovou síť, kterou by pak nemohla využívat jiné zařízení.



Obr. 35.: Stolní počítač Compaq 500B.³⁴

³⁴ ALFA COMPUTER a.s. [online]. 2010 [cit. 2010-05-31]. Compaq 500B. Dostupné z WWW: <<http://www.alfacomp.cz/php/image.php?eid=10F140X4Z&bigimg=55824av.jpg>>.

3.5 Připojení do sítě pomocí smartphone

Připojení do bezdrátové sítě pomocí smartphone je velmi zajímavá možnost a to z důvodu, že kvůli letmému prohlédnutí nějakých informací na internetu, přečtení ranních zpráv u snídaně nebo zkontrolování nových e-mailů, není nutné zapínat stolní PC nebo notebook, což se také může protáhnout.

Smartphone má většina lidí zapnutý pořád a když už je vypnutý, tak trvá pár vteřin jej zapnout a připojit se do sítě. Další výhodou je prakticky okamžité stáhnutí například hudebních souborů z knihovny multimédií, uložených na serveru před cestou do práce. Stejně tak automatické synchronizování kontaktů v telefonu, s databází kontaktů v PC.



Obr. 36.: Nokia N900.

Asi nejlepší volbou v dnešní době je mobilní telefon – tablet Nokia N900. Tento telefon podporuje standard 802.11b/g a na všechny důležité bezpečnostní standardy, jako je WEP, WPA nebo WPA2 má dostatečný výkon.³⁵ S tímto telefonem, by neměl být problém se připojit do dostatečně zabezpečené bezdrátové sítě.

³⁵ Nokia Europe [online]. 2010 [cit. 2010-05-31]. Nokia N900 Tech Specs. Dostupné z WWW: <<http://europe.nokia.com/find-products/devices/nokia-n900/specifications>>.

3.6 Shrnutí všech úprav a rozšíření sítě

Hlavním změnou v síti je přechod od standardu 802.11g na standard 802.11n. Toto vylepšení umožní vyšší maximální přenosovou rychlost sítě. Případné problémy se snižováním výkonu sítě byly vyřešeny následujícím způsobem: bezdrátová tiskárna byla připojena pomocí USB 2.0 do routeru ASUS RT-N16, který podporuje funkci print serveru což znamená, že tiskárnu mohou využívat všichni uživatelé sítě. Připojení notebooku k bezdrátové síti, který nepodporuje standard 802.11n, bylo vyřešeno pomocí rozšiřující karty do ExpressCard slotu D-link Xtreme N Notebook ExpressCard.

Další změnou je přepracovaná infrastruktura sítě. Server byl přesunut do místnosti za kuchyní, kde jsou lepší podmínky pro jeho provoz. Nahrazen byl buď PC sestavou Compaq 500B nebo sestavovaným PC, podle přesných požadavků uživatelů. Server se stal hlavním úložištěm dat celé sítě.

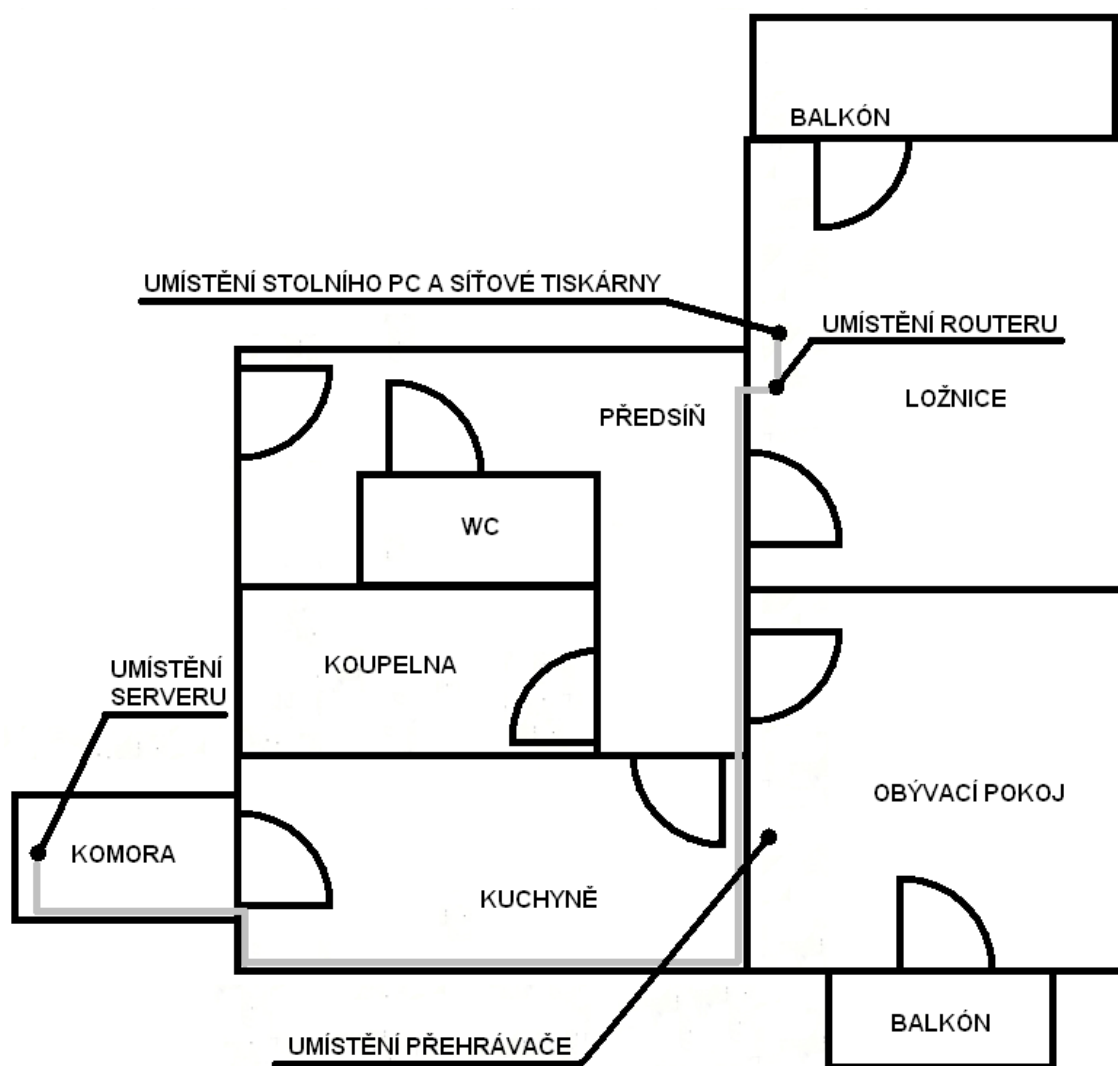
Název zařízení	IP adresa zařízení	Sít'. název zařízení	Popis
ASUS RT-N16	192.168.1.1		Bezdrátový router
Dell Vostro 1500	192.168.1.2	NOTEBOOK	Notebook
Stolní PC	192.168.1.3	PC-DOMA	Domácí PC
HP Photosmart Wireless B109n-z	192.168.1.4		Bezdrátová tiskárna
Popcorn Hour C-200 Blu-ray ready	192.168.1.5	POPCORN-HOUR	Multimediální přehrávač
Server	192.168.1.6	PC-SERVER	Serverové PC
Nokia N900	192.168.1.7	NOKIA-N900	Smartphone

Tabulka 3.: Přehled připojených zařízení po upgradování sítě.

Do sítě přibyl multimediální přehrávač Popcorn Hour C-200 Blu-ray ready, který je vybaven bezdrátovou miniPCI kartou, MikroTik RouterBOARD R52N miniPCI, díky

které se přehrávač může připojit do bezdrátové sítě a je připraven na streamování multimediálního obsahu, ze serveru ve vysokém rozlišení.

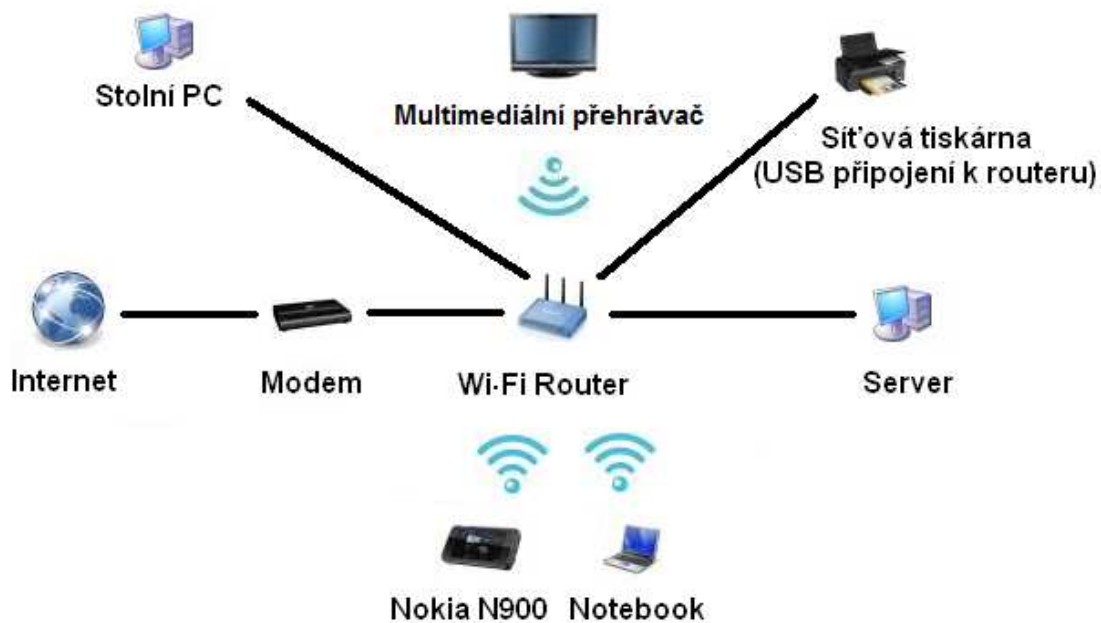
Server byl vybaven možnostmi FTP serveru, pro jednoduchý přístup přes internet, pomocí programu Cerberus FTP Server ke sdíleným datům a složkám. Server je ovládán prakticky výhradně pomocí vzdálené plochy, což ušetřilo náklady na úpravu sítě.



Obr. 37.: Půdorys bytu s vyznačenými umístěními všech pevných prvků sítě.

Posledním zařízením, které se nově připojuje do bezdrátové sítě je smartphone Nokia N900. S tímto zařízením je mnohem jednodušší připojit se k internetu, jen kvůli letmému prohlédnutí nějakých informací, přečtení ranních zpráv u snídaně nebo zkontrolování nových e-mailů. Tento smartphone podporuje standard 802.11b/g a

všechny důležité zabezpečovací technologie - jako je WEP, WPA, WP2. Pro tento smartphone, dokonce existují aplikace, které mu umožňují připojení ke vzdálené ploše, takže s jeho pomocí lze i rychle upravovat nastavení serveru, připojit se ke stolnímu počítači nebo k notebooku.



Obr. 38.: Schéma sítě po aplikaci všech vylepšení.

3.7 Ekonomické zhodnocení

V rámci ekonomického zhodnocení, lze podle mého názoru finančně vyjádřit jen náklady na upgrade sítě. Co týče očekávaných přínosů, bude vyjádření hlavně nefinanční – jejich finanční vyjádření není tak úplně možné.

Po spočítání celkových očekávaných nákladů, dostaneme docela vysokou částku. Doporučil bych tedy, provádět vylepšení sítě postupně v rámci delšího časového úseku. Rozvržení se bude odvíjet od finančních možností daného uživatele.

3.7.1 Očekávané finanční náklady

Pozn.: Ceny jsou vč. DPH a podle ceníku internetového obchodu Alfa Computer³⁶ pokud není uvedeno jinak.

- FTP server – v případě zřízení FTP serveru jsou náklady prakticky nulové. Program Cerberus FTP Server je totiž k nekomerčnímu použití možné využívat zcela zdarma. Jediné náklady, o kterých lze uvažovat jsou náklady nepřímé, jako jsou ceny za energie, potřebné na provoz počítače, na kterém je FTP server spuštěn.
- Připojení TV v obývacím pokoji do sítě – zde jsou náklady již mnohem lépe měřitelné. Přehrávač Popcorn Hour C-200 Blu-ray ready stojí 7490 Kč a Bezdrátová miniPCI karta MikroTik RouterBOARD R52N miniPCI stojí 745 Kč. Náklady celkem jsou tedy 8 325 Kč.
- Zvýšení přenosové rychlosti sítě pro přehrávání 1080p filmů – cena bezdrátového routeru ASUS RT-N16 je 3 155 Kč. Cena rozšiřující karty do ExpressCard slotu D-link Xtreme N Notebook ExpressCard je na stránkách e-shopu D-Link³⁷ 84.99 \$, což je v přepočtu přibližně 1 800 Kč. Celkem tedy 4 955 Kč.

³⁶ ALFA COMPUTER a.s. [online]. 2010 [cit. 2010-05-31]. Internetový obchod. Dostupné z WWW: <<http://www.alfacomp.cz/>>.

³⁷ D-Link - Home & Home Office [online]. 2010 [cit. 2010-05-31]. DWA-643 Xtreme N Notebook ExpressCard. Dostupné z WWW: <

- Umístění serveru – cena Stolní počítač Copaq 500B je 7 850 Kč. Ve chvíli, kdy by se uživatelé rozhodli pro sestavení PC, dá se cena očekávat okolo 20 000 Kč.
- Připojení do sítě pomocí smartphone – cena mobilního telefonu nokia N900 je 14 385 Kč.

Náklady celkem jsou tedy 35 515 Kč, v případě výběru varianty stolního PC, s nižším výkonem a 47 665 Kč při výběru varianty se skládaným PC.

3.7.2 Očekávané nefinanční nákladů

Největšími nefinančními náklady jsou odpracované hodiny, potřebné k úpravě a rozšiřování sítě. V tomto případě počítám s 20 – 25 hodinami práce.

3.7.3 Očekávané nefinanční přínosy

Hlavními přínosy těchto úprav a rozšíření se projevují hlavně ve zvýšení komfortu uživatelů a usnadnění jejich práce. Je otázkou, zda se všechna vylepšení konkrétním uživatelům vyplatí, či nikoliv.

<http://www.dlinkshop.com/DRHM/servlet/ControllerServlet?Action=DisplayProductDetailsPage&SiteID=dlink&CallingPageID=HomePage&ProductID=121988400>>.

Závěr

Tato práce je zaměřena na obecný popis bezdrátové problematiky a Wi-Fi sítí. Snažil jsem se obsáhnout vše důležité v rámci bezdrátové komunikace pomocí Wi-Fi. V teoretické části jsem se snažil popsat nejdůležitější termíny skloňované v bezdrátové komunikaci a to nejenom ty, které se týkají Wi-Fi připojení, ale také důležité termíny týkající se zabezpečení. V poslední části kapitoly **Teoretická východiska** jsem nastínil budoucí vývoj v bezdrátové komunikaci tak, jak si myslím, že by se mohl ubírat.

V další kapitole **Analýza problémů** jsem se snažil popsat mou vlastní bezdrátovou síť. V první části jsem popisoval hardwarové prvky, které používám v mé vlastní síti. V druhé části jsem se zaměřil na popis zabezpečení mé vlastní sítě. Ve třetí části jsem se dostal k samotné analýze problémů, se kterými se v mé síti potýkám.

V poslední kapitole **Vlastní návrh řešení** jsem se snažil, nastínit možnosti řešení problémů, které jsem zmínil na konci předchozí kapitoly. V předposlední části této kapitoly, jsem provedl sumarizaci všech vylepšení sítě. V poslední části je ekonomické zhodnocení.

Tato práce je koncipována tak, aby posloužila jak začínajícím uživatelům, které seznámí s nejdůležitějšími problémy v rámci bezdrátové komunikace, tak i pokročilejším uživatelům, kteří si neví rady s nějakým problémem ve vlastní síti. Měla by také pomoci při návrhu nové sítě, například soukromé domácí sítě, také při jejím sestavování. Touto prací se také mohou inspirovat malé a střední firmy, při vytváření vlastní bezdrátové sítě.

Seznam použitých obrázků

Obr. 1: Logo standardu Wi-Fi.

Obr. 2.: Přehled některých standardů IEEE 802.11.

Obr. 3.: Návrh loga pro zařízení podporující všechny čtyři standardy.

Obr. 4.: Apple Air-Port logo.

Obr. 5.: Apple Air-Port přístupový bod.

Obr. 6.: Rozdělení kanálů (OFDM).

Obr. 7.: Bezdrátový router ASUS WL-500W podporující standard 802.11n.

Obr. 8.: Nastavení filtru MAC adres u bezdrátového routeru ASUS WL-520gC.

Obr. 9.: Zjištění MAC adresy PC pomocí příkazu ipconfig/all.

Obr. 10.: Nastavení skrytí SSID u bezdrátového routeru ASUS WL-520gC.

Obr. 11.: Nastavení zabezpečení WEP u bezdrátového routeru ASUS WL-520gC.

Obr. 12.: Okno programu AirSnort.

Obr. 13.: Nastavení zabezpečení WPA u bezdrátového routeru ASUS WL-520gC.

Obr. 14.: Mechanismus TKIP.

Obr. 15.: Kódování pomocí TKIP, porovnání šifrování ve WEP a ve WPA.

Obr. 16.: Průběh šifrování pomocí AES.

Obr. 17.: Nastavení zabezpečení WPA2 u bezdrátového routeru ASUS WL-520gC.

Obr. 18.: Schéma sítě vytvořené pomocí technologie Smart LED Lighting.

Obr. 19.: Bezdrátový router ASUS WL-520gC.

Obr. 20: Wake On Lan – Magic Packet – utilita na zasílání „Magického Paketu“.

Obr. 21: Ukázka připojení ke vzdálené ploše.

- Obr. 22.: Nastavení přesměrování portů u bezdrátového routeru ASUS WL-520gC.
- Obr. 23.: Webové rozhraní tiskárny HP Photosmart Wireless B109n-z.
- Obr. 24.: Schéma sítě.
- Obr. 25.: Půdorys bytu s vyznačeným umístěním routeru, stolního PC a síťové tiskárny, a silou signálu.
- Obr. 26.: Webové rozhraní bezdrátového routeru ASUS WL-520gC.
- Obr. 27.: Warchalking symboly.
- Obr. 28: Okno programu Cerberus FTP Server.
- Obr. 29: Přehrávač Popcorn Hour C-200 Blu-ray ready.
- Obr. 30: Bezdrátová miniPCI karta MikroTik RouterBOARD R52N miniPCI.
- Obr. 31: Bezdrátový router ASUS RT-N16.
- Obr. 32: Karta do ExpressCard slotu D-link Xtreme N Notebook ExpressCard.
- Obr. 33.: Schéma sítě po zapojení serveru.
- Obr. 34.: Půdorys bytu s vyznačeným umístěním routeru, PC, síťové tiskárny, a serveru.
- Obr. 35.: Stolní počítač Copaq 500B.
- Obr. 36.: Nokia N900.
- Obr. 37.: Půdorys bytu s vyznačenými umístěními všech pevných prvků sítě.
- Obr. 38.: Schéma sítě po aplikaci všech vylepšení.

Seznam tabulek

Tabulka 1.: Přehled připojených zařízení do sítě (k routeru je ještě připojen modem Motorola).

Tabulka č. 2.: Sestava PC Compaq 500B.

Tabulka 3.: Přehled připojených zařízení po upgradování sítě.

Seznam použitých zkratk

ADSL - Asymetric Digital Subscriber Line

AES - Advanced Encryption Standard

AM - Amplitude Modulation

AP - Access Point

CBC-MAC - Cipher Block Chaining Message Authentication Code

CBC-MAC (CCM) - Counter with CBC-MAC

CCMP - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

CDMA - Code division multiple access

CPU - Central Processing Unit

CRC - Cyclic redundancy check

DES - Data Encryption Standard

DSSS - Direct Sequence Spread Spektrum

DVB-T Digital Video Broadcasting - Terrestrial

DVD - Digital Versatile Disc nebo Digital Video Disc

EDGE - Enhanced Data rates for GSM Evolution

EEPROM - Electrically Erasable Programmable Read-Only Memory

FIPS - Federál Information Processing Standards

FM - Frequency modulation

FTP - File Transfer Protocol

GB - Gigabyte

GHz - Gigahertz

GPS - Global Positioning System

GSM - Groupe Spécial Mobile

HD - High-Definition

HDTV - High-Definition Television

HP - Hewlett-Packard

HSDPA - High-Speed Downlink Packet Access

HW - Hardware

IEEE - Institute of Electrical and Electronics Engineers

IP - Internet Protocol

IrDA - Infrared Data Association

IV - Initialization Vector

NIC - Network Interface Controller

LAN - Local Area Network

LED - Light-Emitting diode

MAC - Media Access Control

Mbit/s - Megabit per second

MHz - Megahertz

MIC - Message integrity Code

MIMO - Multiple-input multiple-output

OFDM - Orthogonal Frequency Division Multiplexing

PC - Personal Computer

PCI - Peripheral Component Interconnect

PN - Packet Number

PSK - Pre-Shared Key

QoS - Quality of Service

RC4 - Rivest Cipher 4

SP3 - Service Pack 3

SSID - Service Set Identifier

SW - Software

TB - Terabyte

TC - Total Commander

TK - Temporary Key

TKIP - Temporal Key Integrity Protocol

TV - Television

USA - United States of America

USB – Universal Serial Bus

VPN - Virtual Private Network

WEP - Wired Equivalent Privacy

Wi-Fi - Wireless Fidelity

WiMAX - Worldwide Interoperability for Microwave Access

WPA - Wi-Fi Protected Access

WPA2 - Wi-Fi Protected Access

Seznam použité literatury

- [1] ZANDL, P. *Bezdrátové sítě WiFi: praktický průvodce*. Vyd. 1. Brno: Computer Press, 2003. 190 s. ISBN 80-7226-632-2.
- [2] BARKEN, L. *Wi-Fi: jak zabezpečit bezdrátovou síť*. Vyd. 1. Brno: Computer Press, 2004. 174 s. ISBN 80-251-0346-3.
- [3] BRISBIN, S. *Wi-Fi: postavte si svou vlastní wi-fi síť*. Praha: Neocortex, 2003. 248 s. ISBN 80-291-8644-2.
- [4] BRADÁČ, Z., FIEDLER, P., KAČMÁŘ, M. Bezdrátové komunikace v automatizační praxi I: historie a současnost. *Automa* [online]. 2009 [cit. 2009-12-03]. Dostupný z WWW: <http://www.odbornecasopisy.cz/index.php?id_document=28818>.
- [5] KÖHRE, T. *Stavíme si bezdrátovou síť Wi-Fi*. Vyd. 1. Brno: Computer Press, 2004. 297 s. ISBN 80-251-0391-9
- [6] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace : Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G*. Brno : Computer Press, 2005. 186 s.
- [7] BRADÁČ, Z., FIEDLER, P., KAČMÁŘ, M. Bezdrátové komunikace v automatizační praxi I: historie a současnost. *Automa* [online]. 2009 [cit. 2009-12-03]. Dostupný z WWW: <http://www.odbornecasopisy.cz/index.php?id_document=28818>.
- [8] RAMBOUSEK, Adam. *Fakulta informatiky Masarykovy univerzity* [online]. 2003 [cit. 2010-05-08]. Historie mobilní komunikace. Dostupné z WWW: <http://www.fi.muni.cz/usr/jkucera/pv109/2003/xrambous_index.htm>.
- [9] *MyTselection* [online]. 18.11.2009 [cit. 2010-05-09]. How to choose the right WiFi channel. Dostupné z WWW: <<http://mytselection.blogspot.com/2009/11/how-to-chose-right-wifi-channel.html>>.
- [10] NYGRÝN, Pavel. Wi-Fi zvládne každý!. *Computer*. 24. září 2009, 18/09, s. 6-8.

- [11] *ASUSTeK computer Inc.* [online]. 2009 [cit. 2010-05-09]. WL-500W. Dostupné z WWW: <http://usa.asus.com/product.aspx?P_ID=nrsjewu78wdDXMOA>.
- [12] *Wi-Fi síť Praha* [online]. 2008 [cit. 2010-05-09]. Wi-Fi standard IEEE 802.11. Dostupné z WWW: <<http://prahawifi.cz/wifi-standard-ieee-80211/>>.
- [13] *Linux E X P R E S* [online]. 2007 [cit. 2010-05-13]. Domácí počítačová síť - 2. Dostupné z WWW: <<http://www.linuxexpres.cz/praxe/domaci-pocitacova-sit-2>>.
- [14] *Cisco Systems, Inc* [online]. 2010 [cit. 2010-05-25]. Cisco Unified Wireless Network Architecture - Base Security Features. Dostupné z WWW: <http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch4_Secu.html>.
- [15] *Computer Science at Boston College* [online]. 2010 [cit. 2010-05-28]. AES encryption flash animation. Dostupné z WWW: <http://www.cs.bc.edu/~straubin/cs381-05/blockciphers/rijndael_ingles2004.swf>
- [16] *ASUSTeK computer Inc.* [online]. 2009 [cit. 2010-05-09]. ASUS WL-520gC. Dostupné z WWW: <http://www.asus.cz/product.aspx?P_ID=Pq3TmwugpKCFDkV5>.
- [17] *Pooh.cz* [online]. 2005 [cit. 2010-05-30]. Warchalking a WiFi síť vůbec. Dostupné z WWW: <<http://www.pooh.cz/clanky/warchalking/warchalking.asp>>.
- [18] *ITBiz.cz* [online]. 8.11.2009 [cit. 2010-05-30]. V Praze je zabezpečených 84 % WiFi sítí. Dostupné z WWW: <<http://www.itbiz.cz/praha-zabezpeceni-wifi-pripojeni>>
- [19] *ALFA COMPUTER a.s.* [online]. 2010 [cit. 2010-05-30]. Popcorn Hour C-200 Blu-ray ready. Dostupné z WWW: <<http://www.alfacomp.cz/php/product.php?eid=10514008V000000UTE>>.
- [20] *ALFA COMPUTER a.s.* [online]. 2010 [cit. 2010-05-30]. MikroTik RouterBOARD R52N miniPCI. Dostupné z WWW:

- <<http://www.alfacomp.cz/php/image.php?eid=10F140WFC&bigimg=40491av.jpg>>.
- [21] *ASUSTeK computer Inc.* [online]. 2009 [cit. 2010-05-09]. ASUS WL-520gC. Dostupné z WWW: <http://www.asus.com/product.aspx?P_ID=WAA6AQFncrceRBEo>.
- [22] *D-Link - Home & Home Office* [online]. 2010 [cit. 2010-05-30]. DWA-643 Xtreme N Notebook ExpressCard. Dostupné z WWW: <<http://www.dlink.com/products/?pid=550>>.
- [23] JANEČEK, Vladislav. *Živě.cz* [online]. 19. 5. 2010 [cit. 2010-05-30]. Čínští vědci dokáží vytvořit počítačovou síť z osvětlení v místnosti. Dostupné z WWW: <<http://www.zive.cz/bleskovky/cinsti-vedci-dokazi-vytvorit-pocitacovou-sit-z-osvetleni-v-mistnosti/sc-4-a-152369/default.aspx>>.
- [24] *ALFA COMPUTER a.s.* [online]. 2010 [cit. 2010-05-31]. Compaq 500B. Dostupné z WWW: <<http://www.alfacomp.cz/php/product.php?eid=10514008R000000X4Z>>.
- [25] *ALFA COMPUTER a.s.* [online]. 2010 [cit. 2010-05-31]. Compaq 500B. Dostupné z WWW: <<http://www.alfacomp.cz/php/image.php?eid=10F140X4Z&bigimg=55824av.jpg>>.
- [26] *ALFA COMPUTER a.s.* [online]. 2010 [cit. 2010-05-31]. Internetový obchod. Dostupné z WWW: <<http://www.alfacomp.cz/>>.
- [27] *D-Link - Home & Home Office* [online]. 2010 [cit. 2010-05-31]. DWA-643 Xtreme N Notebook ExpressCard. Dostupné z WWW: <<http://www.dlinkshop.com/DRHM/servlet/ControllerServlet?Action=DisplayProductDetailsPage&SiteID=dlink&CallingPageID=HomePage&ProductID=121988400>>.