

Návrh bezdrátové počítačové sítě v areálu UTB U5

Ladislav Běhal

Bakalářská práce

2005



Univerzita Tomáše Bati ve Zlíně
Fakulta technologická

Univerzita Tomáše Bati ve Zlíně
Fakulta technologická
Institut řízení procesů a aplikované informatiky
akademický rok: 2004/2005

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Ladislav BĚHAL**
Studijní program: **B 3902 Inženýrská informatika**
Studijní obor: **Informační technologie**

Téma práce: **Návrh bezdrátové počítačové sítě v areálu UTB U5.**

Zásady pro vypracování:

1. Zpracujte literární rešerši na dané téma.
2. Zanalyzujte současný stav v oblasti bezdrátových sítí Wi-Fi.
3. Navrhněte několik variant řešení bezdrátové sítě Wi-Fi v areálu UTB U5.
4. Porovnejte navržené varianty z pohledu provozní a finanční náročnosti.

Rozsah práce:

Rozsah příloh:

Forma zpracování bakalářské práce: tištěná/elektronická

Seznam odborné literatury:

1. PUŽMANOVÁ, R.: Širokopásmový internet – Přístupové a domácí sítě. Brno, Computer Press, 2004.
2. ZANDL, P.: Bezdrátové sítě Wi-Fi – Praktický průvodce. Brno, Computer Press, 2003.
3. BRISBIN, S.: Wi-fi – postavte si svou vlastní Wi-Fi síť. Praha, Neokortex, 2004.
4. KÖHRE, T.: Stavíme si bezdrátovou síť Wi-Fi. Brno, Computer Press, 2004.
5. BARKEN, L.: Jak zabezpečit bezdrátovou síť Wi-Fi. Brno, Computer Press, 2004.

Vedoucí bakalářské práce:

Ing. Miroslav Matýsek, Ph.D.

Institut řízení procesů a aplikované informatiky

Datum zadání bakalářské práce:

21. února 2005

Termín odevzdání bakalářské práce:

10. června 2005

Ve Zlíně dne 17. února 2005



prof. Ing. Josef Šimoník, CSc.
děkan



prof. Ing. Vladimír Vašek, CSc.
ředitel institutu

ABSTRAKT

Abstrakt česky

Hlavním cílem této práce je návrh realizace bezdrátového pokrytí fakultní budovy U5 Univerzity Tomáše Bati ve Zlíně.

První, teoretická část je úvodem do problematiky bezdrátových sítí. Jsou zde zpracovány standardy bezdrátových sítí v bezlicenčních pásmech 2,4 a 5,8 GHz. Dále je vytvořen přehled zařízení a využívaných architektur bezdrátové komunikace. Nemalá část teoretické části je také věnována možnostem zabezpečení.

V praktické části je zhodnocen současný stav bezdrátových sítí na fakultní budově U5. Následně je vypracován návrh realizace budoucí sítě. Zde je vytvořeno několik variant zabezpečení, jež jsou výchozím bodem k hardwarovému řešení bezdrátového pokrytí budovy. Dále je navrženo rozmístění a počet přístupových bodů a zpracována cenová kalkulace tohoto řešení.

Abstrakt ve světovém jazyce

The main aim of my bachelor's thesis is the wireless coverage of Thomas Bata University building U5.

The first part offers a theoretical introduction to the topic of wireless networks. Wireless network standards on the licencefree 2.4 and 5.8 GHz frequency band have been dealt with here. Furthermore the introductory part contains an overview of devices and common wireless communication architectures. A chapter of the theoretical part is dedicated to possible security measures.

The practical part evaluates the current state of wireless network in U5 building as well as presents a design proposal of the future network. Several security system alternatives have been proposed here, they are the starting point for the hardware solution of the wireless coverage for this building. The proposal contains also the allocation of access points, number of access points and pricing of this solution.

V rámci této práce bych chtěl poděkovat panu Ing. Miroslavu Matýskovi, Ph.D., za všechny rady a připomínky, který mi velmi pomohly při sestavování této práce.

Prohlašuji, že jsem na celé bakalářské práci pracoval samostatně a použitou literaturu jsem citoval.

Ve Zlíně, 09. 06. 2005

.....

jméno diplomanta

OBSAH

OBSAH	6
ÚVOD.....	8
I. TEORETICKÁ ČÁST	9
1 ÚVOD DO BEZDRÁTOVÝCH SÍTÍ.....	10
2 STANDARDY IEEE 802.11	11
2.1 STANDARD 802.11	11
2.2 STANDARD 802.11B	13
2.3 STANDARD 802.11A	14
2.4 STANDARD 802.11G	15
2.5 STANDARD 802.11F.....	15
2.6 STANDARD 802.11E.....	16
2.7 STANDARD 802.11I	18
2.8 STANDARD 802.11H	19
2.9 STANDARD 802.11C	19
2.10 STANDARD 802.11D	19
3 HARDWARE.....	20
3.1 ACCESS POINTY	20
3.2 MODULÁRNÍ ZAŘÍZENÍ.....	21
3.3 PCI - SÍŤOVÉ KARTY	21
3.4 EXTERNÍ ADAPTÉRY WLAN.....	22
3.5 PCMCIA KARTY	23
3.6 INTEGROVANÉ KARTY WLAN.....	23
3.7 BEZDRÁTOVÉ KARTY PRO PDA	24
3.8 ANTÉNY	24
3.8.1 Rozdělení antén.....	24
3.8.2 Polarizace antén.....	26
3.8.3 Vyzářený výkon.....	27
3.9 KABELY, KONEKTORY, REDUKCE.....	28
3.9.1 Kabely:	28
3.9.2 Konektory:.....	28
3.9.3 Redukce.....	30
3.9.4 Příslušenství	31
3.10 CENOVÁ ANALÝZA SOUČASNÉHO TRHU S VÝROBKY 802.11	31

4	ARCHITEKTURA.....	34
4.1	IBSS.....	34
4.2	SÍTĚ S INFRASTRUKTUROU	34
4.3	BSS/ESS.....	35
4.4	BEZDRÁTOVÉ PŘEMOSTĚNÍ SÍTÍ	35
5	ŠÍŘENÍ SIGNÁLU	37
6	BEZPEČNOST 802.11 SÍTÍ.....	40
6.1	MOŽNOSTI ZABEZPEČENÍ BEZDRÁTOVÉ SÍTĚ.....	40
6.1.1	WEP	40
6.1.2	WPA.....	42
6.1.3	Standard 802.11i	44
II.	PRAKTICKÁ ČÁST	46
7	SOUČASNÝ STAV BEZDRÁTOVÝCH SÍTÍ WI-FI NA U5.....	47
8	NÁVRH BEZDRÁTOVÉ SÍTĚ V AREÁLU UTB U5	48
8.1	ZABEZPEČENÍ	48
8.1.1	Varianta 1: Bezpečnost na základě WEP	48
8.1.2	Varianta 2: 802.11i.....	49
8.1.3	Varianta 3: VPN.....	49
8.1.4	Varianta 4: Systém EDUROAM	51
8.2	HARDWARE	52
8.3	ROZMÍSTĚNÍ A POČET ACCESS POINTŮ	54
8.3.1	Měření propustnosti signálu v lokalitě U5	54
8.3.2	Návrh rozmístění access pointů.....	56
8.4	CENOVÁ KALKULACE	57
8.5	POROVNÁNÍ NAVRŽENÝCH VARIANT	58
	ZÁVĚR	60
	SEZNAM POUŽITÉ LITERATURY.....	61
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	62
	SEZNAM OBRÁZKŮ	64
	SEZNAM TABULEK.....	65

ÚVOD

Pod pojmem „bezdrátové sítě“ je možno shrnout prakticky veškerou bezdrátovou komunikaci počínaje mobilními telefony a televizním vysíláním konče. Naprostá většina bezdrátových sítí je spojena jedním slovem: „licenční pásmo“. V případě potřeby vysílání v tomto pásmu je totiž podmínkou získání (zaplacení) licence. V této práci, však bude pojednáváno pouze o bezdrátových sítích v tzv. „bezlicenčním pásmu“, to bývá také často označováno jako ISM (Industrial Scientific and Medical). Zde je možné vysílat bez nutnosti obdržení licence, což má své klady i zápory (především vznik rušení).

Pokud bude dále v textu řeč o „bezdrátových sítích“, je nutné je chápat jako sítě v bezlicenčním pásmu.

Realizace radiových sítí v bezlicenčních pásmech se v posledních letech stalo běžnou praxí. Díky technologickému vývoji zachycenému v podskupinách standardu 802.11, dochází k masivnímu nárůstu této formy síťové komunikace. Atraktivnost odvětví se ukazuje i na zájmu výrobců prosazovat se na trhu s výrobky umožňující bezdrátovou komunikaci. Trh s těmito zařízeními je v podstatě naplněn do té míry, že je možné při stavbě bezdrátové sítě využít hardwarové řešení několika desítek výrobců.

Naprostému rozšíření bezdrátových sítí brání prakticky jen jejich nedostatečná bezpečnost. Už svojí podstatou totiž nabádají a poskytují prostor k útokům mnohem více, než je tomu u drátových sítí. Nové standardy sice poskytují dostatečnou míru zabezpečení, bohužel však pouze v současné době. V perspektivě několika let bude dnes vybudovaná bezdrátová síť zcela jistě bezpečnostně nevyhovující. Zajištění co možná největší bezpečnosti, je ale při tvorbě bezdrátové sítě nutné dát velký důraz.

V této práci bude navrženo několik variant zabezpečení a následný návrh hardwarového řešení s případným rozmístěním přístupových bodů. Bude také porovnáno řešení z hlediska provozní nebo finanční náročnosti.

I. TEORETICKÁ ČÁST

1 ÚVOD DO BEZDRÁTOVÝCH SÍTÍ

Pod pojmem „bezdrátová síť“ bude v této práci zamýšlen úzký svazek těchto sítí, je tedy záhodno si vysvětlit a rozčlenit bezdrátové sítě jako takové. Bezdrátové sítě lze klasifikovat podle mnoha kritérií. Lze je například rozdělit podle pohyblivosti uživatelů:

- mobilní (umožňují pohyb uživatelů v rámci bezdrátové sítě)
- statické

Statické sítě se vyskytují při bezdrátových přemostěních LAN sítí, nebo při poskytování přístupu do internetu domácnostem.

Podle druhu signálu:

- radiové - Nejčastější druh s dosahem podle použité frekvence. Signály do 1 GHz se šíří jako povrchová vlna (kopírují povrch), signály o vyšších frekvencích (od jednotek GHz) se šíří jako přímá vlna (dosah pouze v rámci optického horizontu).
- optické - Svým dosahem se užívají pro bezdrátové přemostění v rámci sousedních budov. Je nutné zajistit přímou viditelnost.
- infračervené (Sítě s malým dosahem, neprůchozí přes překážky.)

Často se lze setkat i s rozdělením sítí podle pole působnosti. Například označení WLAN (Wireless Local Area Network) se používá pro pojmenování lokálních bezdrátových sítí, nebo osobní sítě WPAN (například za pomoci technologie Bluetooth). WMAN pak označují tzv. „metropolitní bezdrátové sítě“. V této práci bude věnována převážná pozornost WLAN sítím.

Tabulka 1: Rozdělení frekvencí v radiových sítích

Technologie	Mobilní síť	Bezdrátové LAN	Bezdrátové MAN
Frekvence	1,9 a 2,1 GHz	2,4 a 5,8 GHz	10 - 66 GHz

2 STANDARDY IEEE 802.11

IEEE (The Institute of Electrical and Electronics Engineers) sdružuje pod sebe několik set tisíc elektroinženýrů a inamatiků v zhruba 150 zemích. IEEE vydává standardy v mnoha oblastech IT, z nichž nejdůležitější pro bezdrátové sítě v bezlicenčních pásmech jsou od skupiny 802.11.

Před zavedením standardu 802.11 byly bezdrátové přenosy založeny na individuálních řešeních firem, zabývajících se tvorbou spojení mezi specifickými zařízeními (pokladny v hypermarketech, evidenční a skladové systémy ap.). Tyto neměli prakticky žádnou možnost interoperability. Individuální řešení vyžadovalo individuální přístup a znalosti, zabezpečení spočívalo tedy v tom, udržet informace o způsobu přenosu dat v tajnosti.

2.1 Standard 802.11

Standard byl vydán v červenci roku 1997. Definoval tři odlišné fyzické vrstvy a jednu MAC (Media Access Control) vrstvu.

První dvě metody na fyzické vrstvě jsou postaveny na myšlence rozprostřeného spektra, kdy se signál rozprostře na široké pásmo frekvencí. Tak se docílí poměrně slušné odolnosti na rušení, nicméně je to poměrně neefektivní využití přenosového pásma.

První technika nazvaná **DSSS** (Direct Sequence Spread Spectrum), neboli přímo rozprostřené spektrum, předpokládá použití přenosového pásma od 2,412 do 2,4835 GHz, které rozděluje na 14 kanálů (v ČR se využívá 13). Každý kanál má šířku 22 MHz, přitom se vzájemně nepřekrývají vždy jen 3 z nich.. Při odchozím toku dat dochází k přeměně bitů na tok symbolů (symbol = skupina 1 nebo více bitů). Používá se modulační technika **QPSK** (Quadrature Phase Shift Keying), kdy vysílač moduluje nebo násobí každý symbol pseudonáhodnou šumovou sekvencí (tzv. chip). Například pro přenos dat 01, bude „0“ nahrazena sekvencí „10110111000“ a „1“ sekvencí „10110111000“. Pak tedy z původního „01“ vznikne redundantní kód 1011011100010110111000. Při této technice je možné dosáhnout rychlostí 1Mb/s nebo 2Mb/s.

Technika **FHSS** (Frequency Hopping Spread Spectrum), byla vynalezena za druhé světové války, jako řešení na nepřátelské rušení naváděných střel. Metoda rozdělí pásmo do 75 kanálů (každý z nich zabírá 1 MHz). Na těchto kanálech se poté vysílají krátké datové úseky. Po odeslání jednoho úseku se přeskočí na další kanál (čas setrvání max. 20ms), předem určený (podle typu „konverzace“ - tím se snižuje možnost současného použití kanálu). Rychlost je stanovena na 1 Mb/s povinně nebo 2 Mb/s volitelně. Teto metodika umožňuje až 22 lokálních sítí vedle sebe (každou s vlastním pořadím přeskokování)

Poslední specifikovanou metodou je **Diffused Infrared**, neboli přenos pomocí infračerveného záření. Přenos se tedy pohybuje v pásmu 300 - 428 000 GHz. Tato metoda nenašla prakticky využití neboť je omezena několika metry dosahu a dále faktem, že signál neprochází přes překážky, ale naopak se od nich odráží. Rychlost u této metody nepřekročí 2Mb/s.

Na úrovni linkové vrstvy (modelu OSI) nabízí tyto služby:

- Autentizace a deautentizace
- Asociace, disasociace a reasociace
- Bezpečnostní standard WEP (Wired Equivalent Privacy)

Již v době vydání standardu IEEE 802.11 bylo jasné, že do budoucna nebude vyhovovat jeho rychlost, proto se ihned po zveřejnění začalo pracovat na nových - rychlejších standardech. Byly vytvořeny dvě skupiny. Skupina „A“ byla zaměřena na vytvoření nového standardu v jiném frekvenčním pásmu a skupina „B“ pracovala na efektivnějším využití pásma 2,4 GHz.

2.2 Standard 802.11b

„Higher-Speed Physical Layer Extension in the 2,4 GHz Band“

V roce 1999 byl zveřejněn standard 802.11b (zpětně kompatibilní s 802.11), který již používal pouze technologii DSSS. Došlo k zrychlení až k teoretické hodnotě 11Mb/s, praktická rychlost se pohybuje v závislosti na kvalitě signálu do zhruba 6Mb/s (zbytek je pohlcen režii přenosu). Pro dosažení vyšší rychlosti oproti předešlému standardu je použito nové kódování Complementary Code Keying (CCK) spolu s QPSK. Fyzická vrstva podporuje i PBCC (Packet Binary Convolutional Coding), což je proprietární řešení společnosti Texas Instruments nezahrnuté ve standardu 802.11, dovoluje dosáhnout (teoreticky) rychlostí až 22Mb/s nebo 44Mb/s. PBCC je však velmi náchylné na problémy při vzniku tzv. „vícecestných interferencí“ (více v kapitole 4: Šíření signálu) a vyžaduje větší odstup signálu od šumu (SNR). Při přenosu dat se používá poloviční duplex, což znamená, že vysílač buď přijímá nebo vysílá. Dosah je udáván 100 m v budově a řádově kilometry ve venkovních prostorech.

Tento standard přinesl i jednu nevýhodu, a to určitou volitelnost součástí. Proto vyráběné výrobky založené na tomto standardu by nemusely být plně kompatibilní. Naštěstí krátce po zveřejnění tohoto standardu byla založena Wireless Ethernet Compatibility Alliance (dnes již přejmenovaná na: Wi-Fi Alliance), nezisková organizace, která testovala kompatibilitu výrobků založených na standardu 802.11b a udělovala jim známku - Wireless Fidelity (Wi-Fi).

V dnešní době je již tento standard nedostačující, neboť neposkytuje dostatečnou rychlost a bezpečnost.

2.3 Standard 802.11a

„High-speed Physical layer in the 5 GHz Band“

Téhož roku jako u 802.11b (1999) vyšel standard 802.11a. Ten se již pohybuje v licenčním pásmu 5,8GHz na 12 kanálů každý o šířce 20 MHz. Tyto kanály jsou pak rozděleny na 3 skupiny podle výkonu. Čtyři kanály s nejvyšším vysílacím výkonem jsou určeny výhradně pro venkovní použití.

Používá techniku **OFDM** (Orthogonal Frequency-Division Multiplexing), neboli ortogonální multiplex. OFDM je vlastně způsob generování určitého počtu subkanálů, které se vzájemně překrývají. Na nich pak proudí data rychlostí úměrné zarušení konkrétního subkanálu, tím dochází k většímu využití přenosového kanálu a následnému zrychlení oproti 802.11b. Jako modulační technika je používána například QPSK. Technika OFDM se využívá například i u ADSL.

Podle síly signálu a velikosti rušení může běžet v režimech podporujících rychlosti: 6, 9, 12, 18, 24, 36, 48, 54 Mb/s. Užitečná maximální rychlost se pohybuje v rozmezí 30-36 Mbit/s (u nominální rychlosti 54Mbit/s). Díky větší šířce pásma podporuje standard až 8 vzájemně se nepřekrývajících kanálů. Dosah je udáván 20 m v budově a řádově stovky metrů ve venkovních prostorech.

Nevýhodou tohoto standardu je neexistující zpětná kompatibilita se standardy 802.11 a 802.11b (jiné kmitočtové pásmo), nicméně z toho vyplývá i skutečnost, že se vzájemně neruší. Výhodou vyššího přenosového pásma je také to, že v něm neoperují i jiné zařízení, jako například mikrovlnné trouby, bezdrátové zařiz. pro přenos zvuku... Dále je nutno uvést, že ačkoliv je standard již prakticky 6 let starý, stále není možné v ČR používat zařízení ve venkovních prostorech.

2.4 Standard 802.11g

„Higher Speed Physical Layer Extension to IEEE 802.11b“

Standard rozšiřující vlastnosti 802.11b vydaný roku 2003. Pracuje na stejném kmitočtovém pásmu jako 802.11b. Dosahuje podobných rychlostí jako u 802.11a tedy maximálně 54Mbit/s nominálně a zhruba 30 Mbit/s reálně. Zrychlení je způsobeno použitím metodiky rozdělení kanálu pomocí OFDM. Podle síly signálu a velikosti rušení může běžet v režimech podporujících rychlosti: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mb/s

Nižší kmitočet (než 802.11a) způsobuje větší odolnost vůči rušení a větší dosah signálu. Bohužel v reálné praxi bývá zarušení v některých městech způsobené rozšířeností 802.11b na takové úrovni, že výhoda větší odolnosti oproti 802.11a pozbývá významu. Dosah signálu je podobný jako u 802.11b (na stejných rychlostech), ale na konci dosahu signálu dochází k rapidnímu snižování rychlosti.

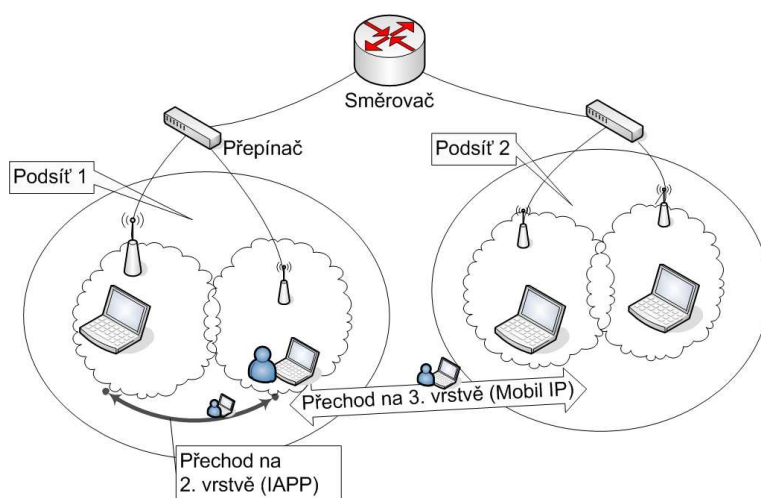
Výkonnost sítě pracující v tomto standardu je podstatně ovlivněna přítomností zařízení na standardu 802.11b. Aby bylo zajištěna možnost koexistence klientů na bázi 802.11b a 802.11g je využívána metoda řízení přístupu k médiu Request-To-Send/ Clear-To-Send (RTS/CTS). Před samotným vysíláním se vysílací strana dotáže access pointu (AP), zda může vysílat (RTS), a ten jakmile je volný vysílací kanál, zašle klientu zprávu o možnosti vysílání (CTS). Tento mechanismus zabezpečuje síť před případnými kolizemi. Pokud však ke kolizi dojde, musí klienti čekat pseudonáhodnou dobu, než opět budou vysílat. Tato doba je však delší u 802.11b než u 802.11g. Tím pádem síť pracující výhradně na 802.11g má kratší dobu čekání než v hybridním režimu. To se významně projevuje v sítích s větším počtem klientů.

2.5 Standard 802.11f

Standard zajišťující interoperabilitu v podpoře přemísťování mezi AP. K **roamingu** dochází, buď na druhé nebo na třetí vrstvě modelu OSI. Na druhé vrstvě se uživatel

přemísťuje v rámci téže podsítě a využívá se zde IAPP (popsaný níže). Pokud dochází k přesunu mimo rámec podsítě, musí dojít i k změně IP adresy klienta. Byl vytvořen protokol síťové vrstvy Mobile IP, který problém řeší prostřednictvím dvou adres: původní a vypůjčené.

Inter Access Point Protocol (IAPP) - V zásadě se jedná o to, že při přístupu na nový access point, musí být původní AP informováno o přesunu klientské stanice.



Obrázek 1: Schéma roamingu

Pro zrychlení roamingu je používáno několik metod:

Key-caching - v autentizačním serveru se ukládají klíče pro opětovné načtení.

Pre-authentication - autentizace předem eliminuje dobu, po kterou je klient odpojen od sítě (lze využívat pouze na druhé vrstvě)

2.6 Standard 802.11e

Původní specifikace pro přístup k přenosovému médiumu 802.11 nenabízela dostatečné zajištění kvality přenosu služeb - QoS (Quality of Service).

Pojem kvalita služby (QoS) vyjadřuje jeden z trendů vývoje technologií a služeb počítačových sítí - poskytovat účastníkům bezdrátové komunikace služby s předem definovanou kvalitou. V současné době se objevují aplikace vyžadující „jistou“ minimální kvalitu přenosu. Jsou to například: IP telefonie, videokonference, internetové televize a další interaktivní služby.

QoS lze definovat několika parametry:

- Zpoždění - doba potřebná k přenosu paketu od odesílatele k adresátovi.
- Ztrátovost paketů - kolik procent paketů nedorazí od odesílatele k adresátovi.
- Chybovost paketů - poměr chybných paketů k celkovému počtu paketů.
- Průchodnost - objem dat v bajtech přenesený za jednotku času.
- Dostupnost služby - rozšířenost signálu v žádaných oblastech.
- Změna zpoždění - jak se mění zpoždění jednotlivých paketů během přenosu.

Standard rozšiřuje přístupy k přenosovému médiumu podle 802.11.

DCF (Distributed Coordination Function)

Je povinnou součástí 802.11 zařízení, založený na metodě CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance). Bohužel však nepodporuje žádné priority přístupu. Tento model řízení přístupu je určen pro asynchronní datové přenosy.

PCF (Point Coordination Function)

- volitelný,
- rozdělení času na dobu „boje o médium“ a dobu „bez boje o médium“,
- nedostatečná podpora priority přístupu (využitelná v době „bez boje o médium“),
- určen pro synchronní přenosy dat, nelze využívat v sítích typu ad-hoc.

Standard 802.11e rozšiřuje stávající metodiky přístupu k přenosovému médiumu. Povinný DCF (rozšíření = EDCF) i volitelný PCF (rozšíření = HCF).

EDCF (Enhanced Distribution Coordination Function)

Každá stanice může mít až čtyři kategorie provozu na podporu osmi úrovních priority. Stanice může vysílat, ale až po intervalu, jehož délka je závislá na úrovni priority. Platí, že čím vyšší priorita, tím menší vyčkávací interval.

HCF (Hybrid Coordination Function)

Přístupový bod se dotazuje stanic v „době bez boje“, zda chtějí vysílat. Pokud stanice odpoví, že ano, AP ji přidělí dobu zahájení přenosu a jeho trvání.

2.7 Standard 802.11i

Nedostatečné zabezpečení bezdrátových sítí v bezlicenčních pásmech vedlo k vytvoření několika bezpečnostních mechanismů, které tuto hazardní situaci mělo zlepšit. Po naprostém neúspěchu zabezpečení pomocí WEP byla uvolněna podmnožina, tehdy ještě nevydaného, standardu 802.11i – WPA (Wi-Fi Protected Access). Dnes se již však implementují bezpečnostní standardy založené čistě na 802.11i.

Standard využívá pokročilé šifrovací standardy TKIP (Temporal Key Integrity Protocol) a AES (Advanced Encryption Standard). Volitelný šifrovací standard (TKIP) vyřešil bezpečnostní nedostatky protokolu WEP. Primární komponentou standardu 802.11i je AES. Tato šifra je náhradou za šifrovací mechanismus WEP/RC4 (WEP je způsob použití šifry RC4). AES šifra již není proudová (lineární) jako RC4, ale bloková (pracuje s bloky o délce 128 bitů).

Bohužel, však šifrování založené na standardu 802.11i je díky blokovému šifrování náročnější na hardware a proto není zpětně kompatibilní se zařízeními postavenými na WEP nebo WPA. Z čehož vyplývá skutečnost, že použití v bezdrátové síti typu hot-spot a podobné, není díky zpětné kompatibilitě realizovatelné.

Větší pozornost bezpečnosti bude věnována v kapitole 5: Bezpečnost 802.11 sítí.

2.8 Standard 802.11h

Tento doplněk se týká pouze 802.11a a tedy zařízení pracující na frekvenci 5GHz. Evropští regulátoři vyžadovali úpravu standardu 802.11a, neboť mohlo u těchto zařízení docházet k rušení některých radarových systémů. Úprava se má týkat dynamického výběru kanálu a omezení vysílacího výkonu.

2.9 Standard 802.11c

Standard schválen roku 1998 upravuje práci komunikačních mostů v rámci MAC.

2.10 Standard 802.11d

V závislosti na individuálních státních možnostech využití bezlicenčních pásem, bylo nutné vytvořit standard pro mezinárodní harmonizaci. Standard schválen roku 2001.

3 HARDWARE

V současnosti poskytují standardy 802.11x poměrně slušnou podporu pro rozvoj bezdrátových sítí. Implementace nových standardů výrobci, však často bývá zpožděná. Najdou se však firmy, které samy řeší některé nedostatky a mezery ve standardizaci. Například fy Cisco, která rozšiřuje bezpečnostní předpoklady svých zařízení. V následující kapitole uvedu stručný přehled zařízení, jež je možno zakoupit na nejen zahraničním, ale již i českém trhu. V konečné fázi této kapitoly je uveden přehled 802.11 produktů na českém trhu.

3.1 Access pointy

Zajišťuje přechod mezi drátovou a bezdrátovou sítí. Access point (AP) obvykle obsahuje port pro připojení drátového zařízení (například routeru), dále konektor pro napájení a konektor pro připojení antény (většinou je od výrobce připojena malá všesměrová anténka) a resetovací tlačítko. Všechny zařízení připojené k AP se musí dělit o šířku pásma. Access pointy jsou limitovány počtem bezdrátových klientů, jež bývá uvedena v popisu produktu od výrobce. Většinou se u nejlevnějších AP (kolem 2000,- Kč) je možno připojit maximálně 6-10 klientů. Nejvýkonnější access pointy podporují až 254 klientů, nicméně 254 klientů má dohromady k dispozici (v případě 802.11b) teoretickou rychlost 11Mbit/s. Takže jeden uživatel, v situaci kdy všech 254 klientů je připojeno, má pouze teoretickou rychlost 43Kbit/s. Navíc při připojení více klientů (zvláště pak u levných zařízení) může docházet k výpadkům, kdy AP přestane reagovat - většinou z důvodu slabé výkonnostní možnosti procesoru (nutný restart AP).



*Obrázek 2: Access point fy
D-Link*

Access point s AP-bridge/wireless bridge

Tyto zařízení jsou rozšířením access pointů o možnosti vytvoření bezdrátového přemostění.

3.2 Modulární zařízení

S rozmachem bezdrátových zařízení přišel i pokles cen a následující rozšiřování funkcí access pointů. V dnešní době existují multifunkční zařízení obsahující přístupový bod i **router** pro směrování přístupu z/do internetu. Často se vyskytují i s **switchem** pro připojení několika LAN klientů nebo s implementací **firewallu** pro zvýšení bezpečnosti proti nežádoucím vniknutím do vytvořené sítě. Integrace **DSL modemu** udělá ze zařízení velmi atraktivní produkt pro vytvoření sítě s možností připojení k internetu.

Je možno se setkat se zařízeními obsahujícími i **tiskové servery** a možnost připojení tiskárny na vyvedený port. Nebo připojení **externího disku** (přes USB) a vytvoření ftp serveru nebo připojení **USB kamery**...

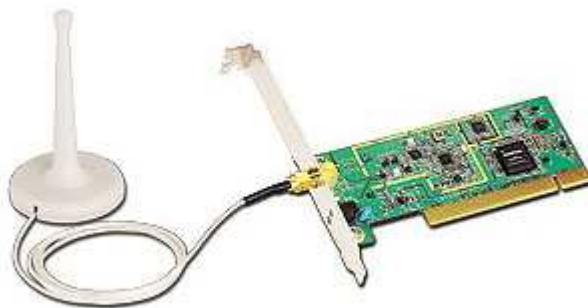


Obrázek 3: Asus 500g -router, ap, switch,...

3.3 PCI - síťové karty

Pro stacionární přístup do bezdrátové sítě se většinou používají karty do PCI. Jsou levnější než access pointy nicméně poskytují menší možnosti. Jednou z nejdůležitějších vlastností PCI karet bývá možnost regulace vysílacího výkonu (pro nepřekročení norem ČTÚ). Tyto karty bývají většinou vybaveny malou anténkou pro přístup do sítí uvnitř budov (indoor sítě). Počítačové skříně bývají často směrované ke zdi, čímž se prakticky znemožňuje

vysílání u antén přímo namontovaných na PCI kartu. Proto výrobci často produkují karty s externí anténkou. Tato anténka není přímo namontována na konektor na kartě, ale vede k ní od konektoru prodlužovací kabel.



Obrázek 4: PCI adaptér

3.4 Externí adaptéry WLAN

Zajímavým řešením převážně pro uživatele s notebooky, jež nemají integrovaný bezdrátový vysílač, je adaptér ve formě USB klíče. Jsou to malé zařízení obsahující integrovanou anténu s nízkým ziskem, jež se zasouvají do USB portu v notebooku nebo PC. Pro USB adaptéry na bázi 802.11b postačuje svou rychlostí USB verze 1.1 (12 Mbit/s), avšak pro přenosové rychlosti 54 Mbit/s (802.11g) je již zapotřebí USB verze 2.0. Existují i speciální antény, dostupné i na českém trhu, které zvyšují dosah USB klíčů. USB klíč se do těchto antén zasune a signál z integrované antény je směřován, tak že dojde k nárůstu signálu v zamýšleném směru.



Obrázek 5: USB stick

3.5 PCMCIA karty

Wireless PC card umístěné do slotu PCMCIA rozšiřují možnosti notebooků o bezdrátovou konektivitu do sítí. Tyto zásuvné moduly bývají většinou vybaveny integrovanou anténou. Jsou však i modely, které mají malou anténu (výjimečně dvě), pro zlepšení úrovně signálu. V poslední době se rozšiřují i antény s konektorem pro připojení externí antény, která však pro mobilní využití není příliš praktická. Konektory bývají proprietárním řešením různých firem například konektory LUCENT (karty Orinoco), pro spojení s externí anténou je nutné zakoupit redukci (tzv. pingtail).

PCMCIA karty je možné využít i do tzv. „wireless ready“ zařízeních, kdy se PCMCIA modul zasune do slotu, například v routeru, a učiní tak z něj bezdrátový router.



Obrázek 6: PCMCIA karta

3.6 Integrované karty WLAN

Implementace bezdrátových technologií do přenosných počítačů se v současné době stala již standardem. Většina dnes již zakoupených notebooků obsahuje integrovanou WLAN kartu postavenou na standardu 802.11g. Výhodou přímé integrace již od výrobce je anténa zabudovaná přímo do konstrukce notebooku, která většinou dosahuje větší ziskovosti než malá integrovaná anténka na USB sticku.

Integrované karty obsahují také dražší verze PDA. Lze předpokládat, že s postupem času bude implementace bezdrátové konektivity standardem.

3.7 Bezdrátové karty pro PDA

Zajímavostí dnešního trhu jsou tzv. wireless SD cards (nebo Wireless Compact Flash Card). Velikosti a použitím naprosto srovnatelné s paměťovými kartami SD nebo Compact Flash. Z miniaturní velikosti vyplývá i výkonnost. Kvůli absenci masivnější integrované antény, dosahují tyto karty minimálního vysílacího výkonu.



Obrázek 7: SD wireless card

3.8 Antény

Antény jsou jedním z prostředků jak umožnit vytvoření bezdrátového spojení na delší vzdálenosti. Použití antén se rozšířilo v ČR hlavně díky unikátní situaci v dostupnosti internetové konektivity z hlediska komerčního využití. V západních státech je pojem wi-fi převážně považován za prostředek k vytvoření tzv. indoor sítí, tzn. sítí uvnitř budov. Kdežto u nás v ČR jsou bezdrátové spoje nejčastěji využívány v outdoorových sítích a to v „poslední míli“ poskytování konektivity do internetu (tzv. wi-fi provider). V současné době je možno vybírat z širokého spektra antén usměrňujících signál na standardech 802.11x. Při výběru antény je nutné brát zřetel na to, pro které frekvenční pásmo ji chceme (2,4GHz nebo 5,8GHz).

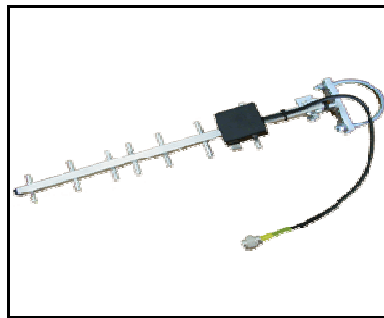
3.8.1 Rozdělení antén

Antény lze dělit podle směru distribuce signálu:

- směrové
- všesměrové
- sektorové

Směrové:

Tyto antény se vyznačují malým vyzařovacím a větším ziskem. Jsou určeny většinou pro klienty a spoje typu peer-to-peer. Tyto antény se vyskytují v rozličných formách například: parabolické síto (vyznačující se velkým předozadním poměrem vyzařování, častým nekvalitním provedením), yagi (lepší předozadní poměr než par. síto)



Obrázek 8: Směrová yagi anténa

Sektorové:

Pokrývají určitý oblastní sektor. U antén je udáván vyzařovací úhel typicky od 60 do 180 stupňů. Vertikální úhel je lepší než u všesměrových antén (je možno pokrýt i místa blízké dolní části vysílače). Využití těchto antén je převážně k poskytování signálu u access pointů.



Obrázek 9: Sektorová anténa

Všesměrové:

Vyzařují v horizontálním úhlu 360° , vertikálním 10 - 20 stupňů. Nízký vertikální úhel způsobuje nemožnost pokrytí signálem oblast v těsné blízkosti pod vysílačem. Všesměrovost vysílání se využívá u access pointů. Tyto antény jsou levnější variantou k několika sektorovým anténám umístěných tak, aby pokryly danou oblast do všech směrů.



Obrázek 10: Všesměrová anténa

3.8.2 Polarizace antén

Polarizace je v podstatě směr vyzařování paprsků. Rovina polarizace vyzářeného vlnění je dána výhradně konstrukčním uspořádáním antény. Polarizaci musí zvolit obě strany (AP i klient) stejnou, neboť v opačném případě by bylo přijímání bráno pouze jako šum. Přesněji při opačné lineární polarizaci dochází k útlumu signálu zhruba o 16 až 24 dB, naproti tomu při použití antény s kruhovou polarizací a antény s lineární polarizací vykazuje spoj pokles signálu pouze o 3 dB.

U antén rozlišujeme 3 typy polarizace:

- lineární vertikální
- lineární horizontální
- kruhová polarizace

Lineární vertikální:

Sinusoida se pohybuje se shora dolů a nazpět. Tato polarizace je nejběžnější, často taky jediná, kterou umí tradiční všesměrové antény (všesměrová anténa složená z více sektorových antén může být přepnuta i do horizontální polarizace).

Lineární horizontální:

Kdy se sinusoida vlny pohybuje z leva doprava a nazpět. Tato polarizace se často využívá u směrových spojů. Výhodou této polarizace je často menší zarušenost (vertikální a horizontální polarizace se navzájem téměř neruší). U směrových antén lze docílit horizontální polarizace pouze natočením antény od 90°.

Kruhová polarizace:

Rozlišujeme pravotočivou a levotočivou kruhovou polarizaci. Sinusoida se točí do spirály - je spojením vertikální a horizontální polarizace. Tato polarizace je nejvíce odolná proti rušení, nicméně je nutné poznamenat, že svojí podstatou (vertikální+horizontální polar.) ruší spoje obou lineárních polarizací.

3.8.3 Vyzářený výkon

Zisk je vlastně poměr intenzity vyzařování v daném směru k poměru intenzity vyzařování do všech směrů tzv. izotropní anténou (matematická anténa vyzařující do všech směrů stejně, tzn. její vyzařovací diagram je koule). Jednotkou zisku antény je pak dBi (i = izotrop). Také se udává ziskovost antény v dBd, což je vlastně hodnota zisku antény vztažená k dipól anténě (tvar T). Nejčastěji však výrobci udávají zisk v dBi, zřejmě protože je o 2,16 větší než hodnota v dBd.

Maximální hustota vyzářeného výkonu daná ČTÚ (Českým telekomunikačním úřadem) je stanovena tak, že hustota vyzářeného výkonu antény nesmí překročit hustotu vyzářeného výkonu izotropní antény s zařízením o výkonu 100 mW (což je vlastně $1020/10 \text{ mW} = 20 \text{ dBm}$).

Volbu antény může ovlivnit i například nehomogenita prostředí, ve kterém se bude signál od antény šířit. Nejvíce náchylná na nehomogenitu jsou antény s převládajícím rozměrem v jednom směru (například yagi anténa).

3.9 Kabely, konektory, redukce

3.9.1 Kabely:

Propojení WLAN adaptéru s anténou je nutné pomocí speciálních nízkoútlumových vysokofrekvenčních kabelů.

Za parametry kabelů lze považovat:

- Impedanci (Ω)
- Útlum (dB/m)
- Průměr (mm)

Dalším méně často uváděným parametrem je „minimální poloměr ohybu“ - je to údaj (většinou kolem 10 cm), který je mezní hranicí pro úhel ohybu. Při ostřejším úhlu dojde k prudkému nárůstu útlumu.

Pro přenos signálu v pásmu 2,4 GHz jsou používány kabely s impedancí 50 Ω . Je možno použít i s odporem 75 Ω , ale pak je nutné připočíst při každém přechodu z 50 na 75 Ω příslušný útlum. Kabely jsou vyráběny v mnoha provedeních vyznačující se hodnotou útlumu na metr (dB/m). Kabely se liší použitým dielektrikem (většinou bývá polyethylenové, nebo vzduchové) a průměrem středního vodiče. Stínění bývá většinou provedeno hliníkovou fólií a měděným opletením. Jako příklad VF kabelu uvedu coax. kabel Belden H1000 PE s útlumem 21dB/100m (orientační cena 46,- Kč/m).

3.9.2 Konektory:

V současné době existuje několik typu konektorů (bohužel není pouze jeden). Nejvýznamnější konektory jsou: N, SMA a Lucent. Konektory je možné také rozdělit podle způsobu připevnění na kabel. Jsou konektory šroubovací nebo tzv. krimplovací. Nejčastěji používané jsou krimplovací, kdy se speciálními kleštěmi zalisuje stínění kabelu mezi konektor a krimplovací kroužek. Konektor se většinou zabezpečuje proti vniknutí vlhkosti obalením vulkanizační páskou.

N konektory:

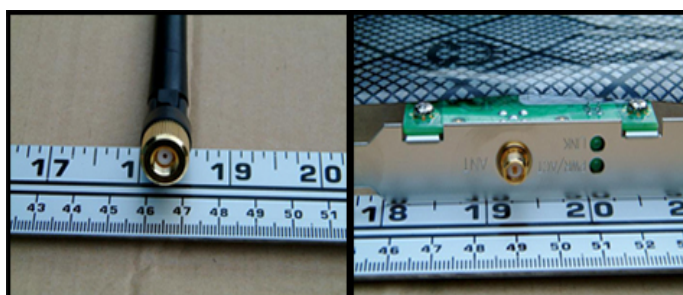
Svou masivní konstrukcí jsou typické pro zapojení na kabelech směřujících od antény. Mají útlum kolem 1dB. Tyto konektory vyhovují až do frekvence 10 GHz. Značkové konektory se vyznačují kvalitními dlouhou životností (10 let), vodotěsností a bezesporu vysokou cenou, která se může pohybovat kolem 400,- Kč. Levnější neznačkové konektory se kvalitativně v některých případech téměř neliší od značkových, ale lze je pořídit v cenové relaci kolem 100,- Kč.



Obrázek 11: N female, krimpovací konektor

SMA konektory:

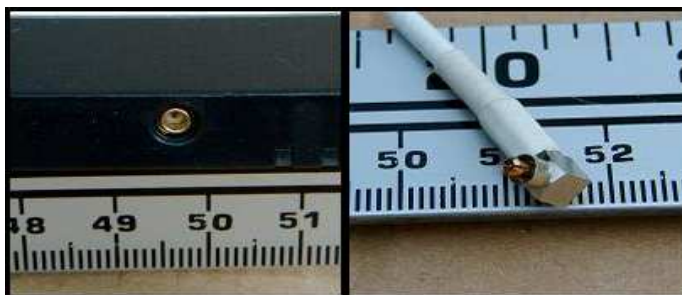
Ve srovnání s N konektory jsou SMA konektory podstatně menší, svojí velikostí jsou totiž uzpůsobeny konektorům na PCI WLAN adaptérech nebo access pointech. Často se však neseťkáváme s konektory SMA, ale reverzními SMA (RSMA), které se liší od SMA konektorů pouze tím, že mají opačně zapojenou dutinku a středový kolík.



Obrázek 12: RSMA Female a Male konektor

Konektory Lucent:

Tyto konektory jsou používány u PCMCIA karet Orinoco. Konektory Lucent jsou pouze proprietárním řešením jedné firmy. Je mnoho dalších konektorů od jiných firem vyžadujících propojení s anténou pomocí redukce.



Obrázek 13: Female a Male konektor Lucent

3.9.3 Redukce

Pro propojení adaptéru s anténou, které mají různé typy konektorů je nutno použít redukce (slangově: pigtaily). Ty často bývají v krátkém provedení (několik desítek cm). Pigtaily se většinou prodávají i v provedeních přímo pro určité adaptéry. Například redukce k bezdrátovým prvkům firmy Linksys, kdy na jedné straně je reverzní TNC Female konektor a na druhé konektor N-Female (pro připojení antény, bleskpojistky...). Ceny pigtailů se pohybují ve stovkách korun. Je možno zakoupit i T redukce nebo redukce ve formě spojky. Na prodloužení již stávajícího kabelu. Zajímavou možností jsou také anténní rozbočovače, díky nimž lze připojit na jeden access point více antén.

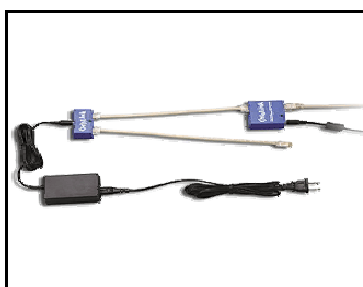


Obrázek 14: Pigtail

3.9.4 Příslušenství

Jako ochrana proti blesku jsou používány tzv. bleskpojistky, které mimochodem nejsou většinou koncipovány na úder blesku, ale pouze na vzniklé rázy v blízkosti úderu. Bleskpojistky jsou významným útlumovým členem spoje adaptér→anténa.

Zajímavostí příslušenství k bezdrátovým zařízením jsou tzv. PoE (Power over Ethernet), kdy se vede elektrické napětí po ethernetovém kabelu z důvodů nedostupnosti elektrické energie v místě vysílače. Teoreticky je možné dosáhnout přemostění vzdálenosti až 100m (při použití kabelů Cat. 5).



Obrázek 15: PoE pro AP

Ovis 1120

3.10 Cenová analýza současného trhu s výrobky 802.11

Dostupnost zařízení nutných k vybudování bezdrátové sítě, lze považovat za více než dostatečnou. Pro získání přehledu o současných (květen 2005) cenových relacích je uveden následující rozbor. Ceny byly získány získával z cen obchodů na www.i4shop.net, www.aspa.cz a www.wifishop.cz. Budu je uvádět bez DPH (19 %), protože škola jako nezisková státní organizace není plátcem daně z přidané hodnoty.

WLAN adaptéry do sběrnice PCI je možno pořídit i za necelých 600,- Kč. Ovšem v tomto případě se bude jednat o výrobek tzv. „neznačkových výrobců“, který často nemá dostatečnou podporu zabezpečení, nových firmwaru, atd. Také se vyskytují duální karty,

práceschopné v obou frekvenčních pásmech. Jednou z těchto karet je D-link DWL-AG520 (zhruba za 2 000,- Kč).

Access pointy jsou podle své vybavenosti prodávány v cenové relaci od 1 200,- (OvisLink WL-1120AP) do ceny pohybující se v desetitisících. Zajímavý access point firmy Orinoco AP-4000 802.11a/b/g, který může pracovat v duálním režimu, podporuje zabezpečení dle IEEE 802.11i a AES, může provozovat až 16 separátních VLAN, podporuje QoS, umožňuje automatickou volbu kanálu (podle zarušení) a mnohé další zajímavé funkce. Cena tohoto výrobku se na českém trhu pohybuje zhruba kolem 12 500,- Kč.

PCMCIA karty se dají koupit od 600,- Kč do ceny několika tisíc korun. Cenově se většinou liší podle podporované rychlosti a možnostech zabezpečení. Nejdražší moduly jsou připraveny na podporu 802.11i, proto musí mít větší výkonový systém než karty podporující pouze WEP.

USB klíče se prodávají zhruba od 1 000,- Kč (pouze 802.11b) a výše, kdy cenu ovlivňují parametry bezpečnosti, rychlosti přenosu a vysílacího výkonu.

Antény a jejich ceny je nutno brát se zřetelem na použití. Indoor (vnitřní) antény se cenově pohybují od 600,- Kč až do 2 000,- Kč. Ziskovost těchto antén se pohybuje kolem hodnot 5-10 dBi. Klientské venkovní antény se ziskovostí 10-14 dBi stojí většinou kolem tisíce korun. Profí antény jsou samozřejmě kvalitou a cenou v jiné kategorii. Je možné zakoupit profí sektorové antény za několik tisíc korun (2 000,- až 5 000,- Kč). Ovšem existují i speciální antény (například s různým vysílacím ziskem a přijímacím ziskem). Takovéto antény se cenově mohou vyšplhat až na statisíce korun.

Cena kabelů je většinou kolem 50,- Kč za metr, konektory stojí zhruba 100,- Kč. Existují i další síťová zařízení například ip kamery (ty se pohybují řádově v tisíci korunách), nebo wi-fi zařízení typu ASUS WL-HDD, které je prakticky jen šuplík pro harddisk pracující v bezdrátovém režimu jako AP, síťový most nebo ftp server (cena zhruba 3 200,- Kč).

Tabulka 2: Orientační ceny

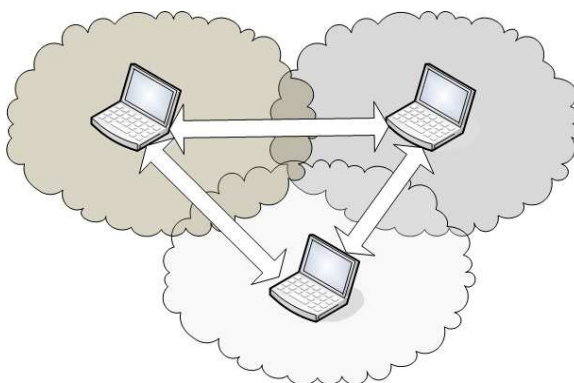
Zařízení	Ceny	
	Od	Do
PCI adaptéry	600 Kč	2 000 Kč
PCMCIA adaptéry	600 Kč	3 000 Kč
USB klíče	1 000 Kč	2 000 Kč
Access pointy	1 200 Kč	30 000 Kč
Antény	600 Kč	5 000 Kč
Kabely	45 Kč	300 Kč

4 ARCHITEKTURA

Síť využívající jako přenosové médium vzduch se prakticky (s určitou formou představivosti) neliší od sítí uskutečňujících přenos po pevných, metalických nebo optických, drátech. Vždy je zapotřebí síťové karty, případně nějakého rozbočovače, mostu... Existuje několik možností jak koncipovat bezdrátovou síť, jež popíši v následujících kapitolách.

4.1 IBSS

Tyto sítě se často označují také pojmem Ad-hoc (ihned). Jejich výhodou je, že nepotřebují žádný AP. Pracují totiž v režimu p2p (peer-to-peer). V této síti, každý uzel (WLAN adaptér) funguje zároveň jako klient a směrovač. Dosah sítě je vytvářen prakticky tím, že každý účastník svůj dosah přidá k již stávajícímu.



Obrázek 16: Ad-hoc síť

Ad-hoc sítě jsou využitelné prakticky jen v situacích, kdy je potřeby rychlého vytvoření bezdrátové sítě (konference). Z architektury je zřejmé, že výkonnost ad-hoc sítí rapidně klesá s vytvořením tzv. skrytého uzlu, kdy vysílací strana nevidí na přijímací a z toho důvodu musí data být směrována přes ostatní účastníky ad-hoc.

4.2 Síť s infrastrukturou

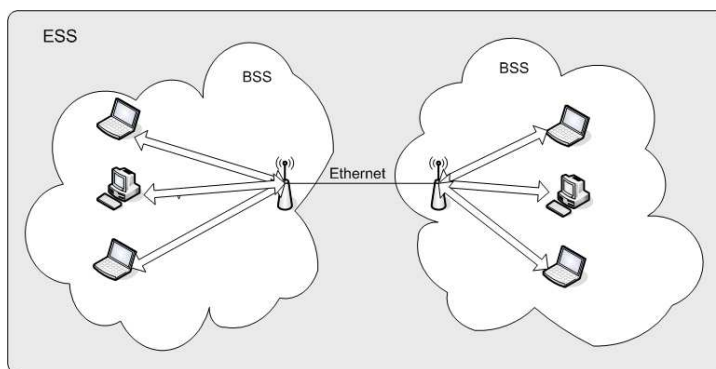
V sítích s infrastrukturou figurují vždy klienti a minimálně jeden access point. Klienti nekomunikují přímo mezi sebou, ale komunikace je zprostředkována přes centrální bod.

4.2.1 BSS/ESS

Basic Service Set (BSS) - je vlastně přenos informací přes jeden access point, kdy veškerá komunikace je směřována přes tento centrální bod.

Extended Service Set (ESS)- je propojení více BSS sítí přes distribuční systém (například Ethernet).

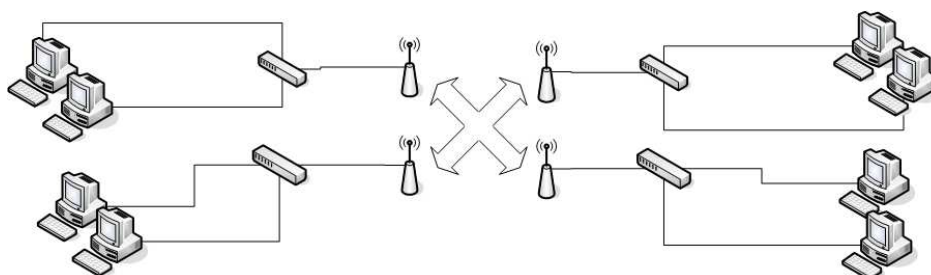
V ESS síti je možné přecházet přes jednotlivé oblasti signálu access pointů (tzv. roaming).



Obrázek 17: BSS/ESS síť

4.3 Bezdrátové přemostění sítí

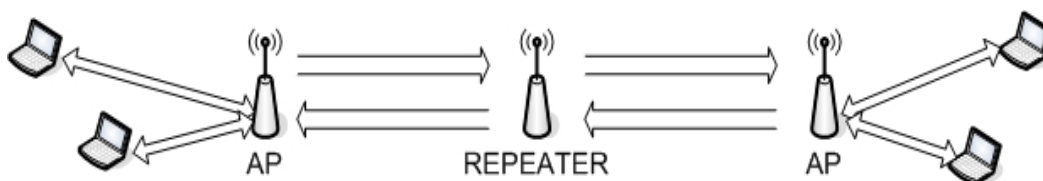
Někdy je zapotřebí přemostit drátové síť pomocí technologie 802.11. Toho se docílí pomocí spojů typu **point to point bridge**, kdy je nutné na access pointu (podporujícím tento mód) zadat MAC adresu protějšího bodu, AP musí mít stejné SSID (identifikátor radiové sítě) a pracovat na stejném přenosovém kanálu. Rozšířeným módem je **point to multipoint bridge** umožňující propojení více než dvou kabelových sítí.



Obrázek 18: Point to multipoint architektura

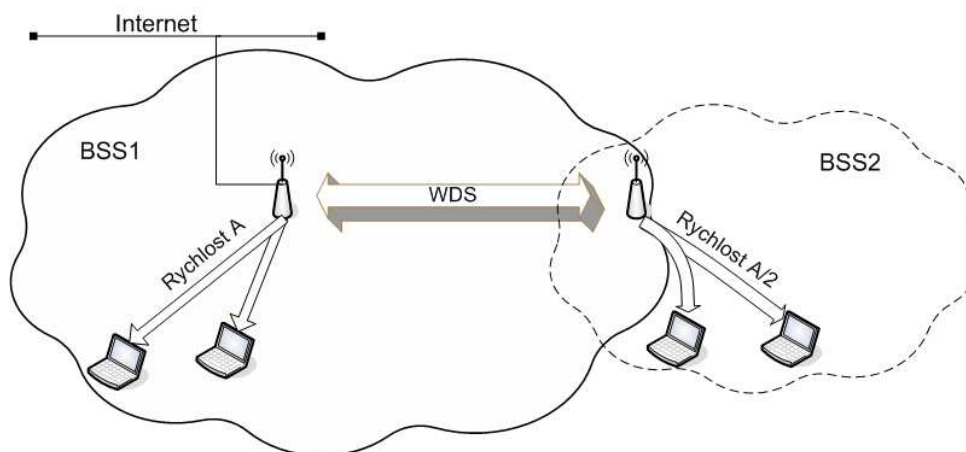
Existuje i řešení nazvané **point to multipoint s infrastrukturou**, což je vlastně nahrazení kabelové sítě (drátových přepínačů) bezdrátovou infrastrukturou (access pointy).

Při nedostatečné možnosti pokrytí pro přemostění sítě pomocí point to multipoint struktury je nutné použít access point v módu **repeater**.



Obrázek 19: Struktura sítě s repeaterem

Je možné rozšířit síť propojením více access pointů přes metalickou síť nebo nastavit přístupové body do **hybridního režimu** (tzv. WDS - wireless distribution system), kdy AP pracuje zároveň jako klient pro přemostění komunikace a centrální jednotka pro určitou podsíť. Nicméně je nutno podotknout, že práce v hybridním módu je limitována počtem AP (většinou je udáván max. počet 8 AP). Hybridní mód totiž způsobuje zpomalení, které je po několika „přeskocích“ na kritické úrovni. Rychlost se totiž snižuje při každém „přeskoku“ o zhruba polovinu. Toto řešení stále není standardizováno, proto se vyskytují u výrobců odlišující se metodiky. Z toho plyne nutnost plánování stavby sítě na základě výrobků od jednoho výrobce (nejlépe stejné řady firmwaru).



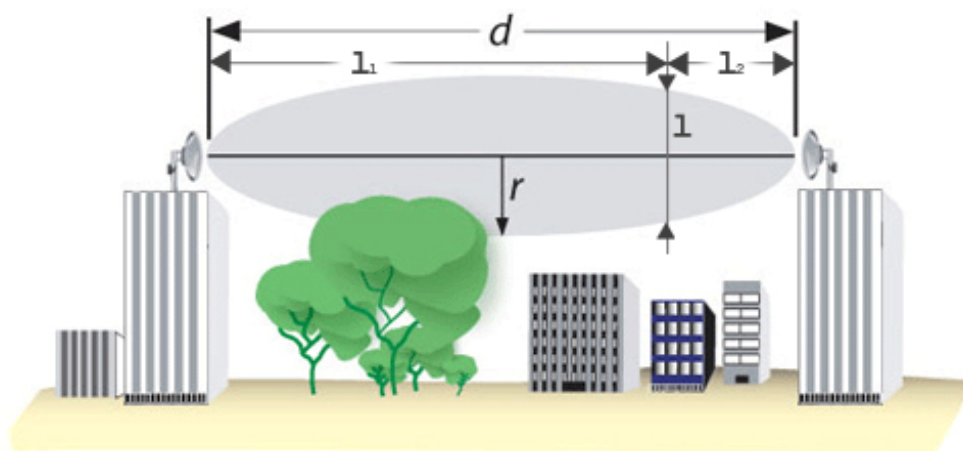
Obrázek 20: Ukázka WDS sítě

5 ŠÍŘENÍ SIGNÁLU

Charakteristika šíření radiového signálu o frekvenci 2,4 GHz je často proklamovaným tématem nejen knih, ale i diskusních fór. Často se setkáváme s názory, že šíření signálů je naprosto nelogické a není možno ho odvozovat podle matematicko-fyzikálních vztahů. Opak je pravdou, protože se často zapomíná brát zřetel na zdánlivě nepodstatné faktory, které se často podepíší dostupnosti bezdrátového signálu.

Nejznámější nutností pro vytvoření bezdrátové komunikace je přímá viditelnost. Samozřejmě, že při realizaci sítě uvnitř budovy nelze předpokládat, že veškerá komunikace bude probíhat pouze v rámci přímé viditelnosti. Při přestupu z jednoho prostředí (vzduch) do druhého (zeď) dochází k velkému snížení intenzity signálu. Jednou z nejhorších překážek pro šíření radiového signálu jsou železobetonové zdi (železné pruty uvnitř zdiva).

Při realizaci ve venkovních sítích musíme dbát na přímou viditelnost s důrazným zřetelem na **1. Fresnelovu zónu** (čtete Frenelova). Převážná část, zhruba 90%, energie se totiž šíří v jakémsi elipsoidu (slangově často nazývaným „doutník“). Pokud dojde k narušení této zóny (nebude v celém svém objemu homogenní), dojde k výraznému snížení kvality signálu. Za 100% porušení se považuje překážka, která zasahuje od spodního okraje do pomyslné přímky z bodu vysílače do bodu přijímače. Při 100% narušení dojde k poklesu kvality signálu na 18%. Většina literatury udává, že k dosažení uspokojivého spojení je nutno mít 60% Fresnelovy zóny bez překážek.



Obrázek 21: Fresnelova zóna

Výpočet šířky Fresnelovy zóny je možné pomocí vzorce:

$$l = \sqrt{\lambda \frac{l_1 l_2}{l_1 + l_2}} \quad (1)$$

l = šířka elipsoidu [m],

l_1, l_2 = vzdálenosti od vysílače, přijímače [m]

λ = vlnová délka frekvence přenosu [m]

$$\lambda = \frac{c}{f} \text{ [m]} \quad (2)$$

c = rychlost světla [m/s],

f = frekvence [Hz]

Často se stává, že v oblasti Fresnelovy zóny jsou stromy, ty bývají často podceňovány co do rušivosti. V zimě, když jsou stromy holé je ztrátovost signálu prakticky minimální, pokud se však v létě listy orosí nebo začne pršet, vznikne téměř nepropustná clona, která znemožní průnik signálu. Energie vlny totiž rozkmitává molekuly vody a tím ji ohřívá (signál je pohlcován). Tento princip je mimochodem využíván v mikrovlnných troubách (pracujících ve stejném pásmu jako wi-fi). Markantní pokles signálu při dešti může nastat u zařízení pracujících na frekvenci 5,8 GHz, kdy dochází k útlumu až 0,5 dB/km (pro 2,4 GHz je zhruba 10x menší).

K dalšímu, nikoli však méně významnému, úbytku signálu dochází vlivem **vícecestné interference**. Při tomto jevu dochází v přijímači ke skládání téhož vyslaného signálu z vysílače. Vlivem odrazu se totiž tentýž vyslaný signál dostane do přijímače v různých časových okamžicích (podle délky trasy). Časový rozdíl mezi prvním signálem (který se šířil po přímce vysílač-přijímač) a posledním signálem je nazýván delay spread (rozprostřené zpoždění). Nejvyšší možné zpoždění je udáváno cca 500 ns, pro plnou rychlost (u 802.11b) je však pouhých 60ns. Největší zpoždění bývá zaznamenáváno uvnitř

v indoor sítích, kdy se signál odráží od mnoha překážek. Tento problém bývá řešen u access pointů pomocí dvou antén (vždy je používána podle kvality signálu jen jedna).

Na kvalitě obdrženého signálu se podepisuje také rušení od ostatních zařízení v pracovním pásmu bezdrátového spoje. Nejvíce dochází k rušení od jiných wi-fi nebo wi-fi5 sítí pracujících na stejném kanále (pro 802.11b jsou pouze 3 nepřekrývající se, 802.11a jich má 8). Je možné i rušení od bezdrátové komunikace založené na technologii Bluetooth, nicméně vzhledem k faktu, že tyto sítě se vyznačují metrovými dosahy, lze tyto možné interference většinou pominout. Často je možné se setkat s dotazy, zda může rušit signál mikrovlnná trouba. Pravdou je, že za určitých okolností je možné připisovat jistý podíl rušení o několik řádů vyššímu vysílacímu výkonu mikrovlnné trouby. Vzhledem k tomu, že prakticky nikdo nezapíná troubu s otevřenými dvířky a k faktu, že mikr. trouby se vyznačují dobrým stíněním, je však rušení v praxi minimální.

Při realizaci bezdrátového spoje na delší vzdálenosti je jedním z nejdůležitějších vztahů vztah na výpočet ztráty signálu ve volném prostoru. Lze ho vyjádřit vztahem:

$$L_p(\text{dB}) = 92,45 + 20 * \log(10 * f) + 20 * \log(10 * d) \quad (3)$$

L_p = ztráta vzniklá na přenosové trase [dB]

f = frekvence [GHz]

d = vzdálenost vysílače od přijímače [km]

6 BEZPEČNOST 802.11 SÍTÍ

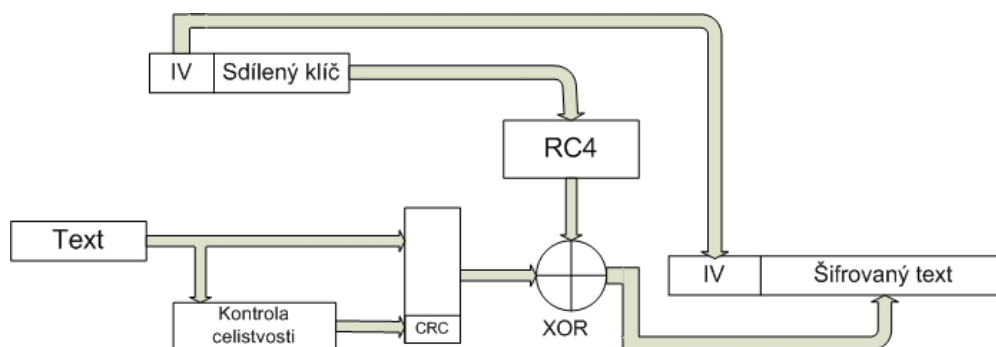
Bezdrátové sítě používají jako distribuční médium volný prostor, je nasnadě tedy nasnadě upozornit na bezpečnostní kritéria s tím spojené. Signál šířený bezdrátovým spojem, se šíří nejen do prostorů námi chtěných, ale i mimo zamyšlenou oblast konektivity. Často je možno se setkat s názorem, že možnost připojení do WLAN sítě, končí za úrovní (v případě indoor sítí) stěn budovy. Toto ovšem, již z podstaty šíření často nebývá pravdou. Navíc existují antény díky nimž lze odposlouchávat sítě na vzdálenost desítek kilometrů. S případnou nechtěnou infiltrací do sítě je nutno počítat a v případě nutnosti se ji snažit i zabránit. Málo zabezpečené sítě bývají napadávány infiltrátory a označovány jako možné připojení. Těmto aktivitám se v zahraničí říká „war-chalking (válečné křídování)“. V současnosti jsem se setkal s těmito aktivitami i na českém internetu, kde bylo popisováno jakými značkami mají označovat lokality s možným přístupem do WLAN sítě. K zamezení nechtěné infiltrace do WLAN sítě je používáno několik technik, které se pokusím nastínit v následujících kapitolách.

6.1 Možnosti zabezpečení bezdrátové sítě

6.1.1 WEP

Tento bezpečnostní protokol, uvedený ve specifikace 802.11b, byl vytvořený na základní ochranu proti infiltraci. Měl vytvořit srovnatelnou ochranu s drátovými sítěmi - proto název Wired Equivalent Privacy. Proces šifrování probíhá tak, že se nejprve vypočítá kontrolní součet (CRC) k šifrovanému textu a se připojí němu. Jako druhou fázi lze brát připojení tajného klíče k inicializačnímu vektoru. Inicializační vektor a tajný klíč se v generátoru pseudonáhodných čísel v šifře RC4 překombinují do tzv. „šifrovacího klíče“. Nonekvivalencí šifrovacího klíče s šifrovaným textem získáme zašifrovaný text. Šifrovací klíč bývá 40, 104, 232 bitů dlouhý. Inicializační vektor (IV) má délku 24 bitů. Před zašifrovaný text se připojí inicializační vektor (ten je zapotřebí k následné dešifraci textu). Dešifrování probíhá obdobně jako šifrování. Vezme se inicializační vektor připojený k zašifrované zprávě a ten se spolu s tajným klíčem předá RC4. S výsledkem z generátoru a šifrovanou zprávou se pak provede XOR (nonekvivalence).

Průběh šifrování ilustruje následující obrázek.



Obrázek 22: Princip WEP šifrování

Opakovaným použitím inicializačního vektoru protokol WEP naráží na jeden ze svých majoritních nedostatků. Inicializační vektor je totiž 24 bitová hodnota, která se při velkém provozu na síti „vyplývá“ již za pár hodin. Nedostatek je v tom, že generátor pseudonáhodných čísel RC4 (proudová šifra použitá například i v SSL) potřebuje ke svému bezchybnému běhu pokaždé různou hodnotu inicializačního vektoru, jinak RC4 generuje stejnou hodnotu šifrovacího klíče. To vede k různým možnostem rozšifrování textu.

Dalším problémem je průběh autentizace. Standard 802.11 rozlišuje dvě metody autentizace **Open system** (otevřený systém - nulová bezpečnost, nutné znát pouze SSID) a **Shared key** (sdílený klíč), kdy se v první řadě zašle od access pointu 128 bajtů dlouhá výzva, kterou klient žádající o autentizaci zašifruje. V případě úspěšného ověření na straně access pointu dojde k autentizaci klienta. Pokud tuto komunikaci útočník zaslechne, může XORem výzvy a odpovědi získat šifrovací sekvenci, kterou použije při vlastní podvržené autentizaci.

Z předešlých řádků je celkem jasné, že bezpečnost zajištěná protokolem WEP je velmi strohá, neřkuli nedostačující. Navíc na internetu je mnoho návodů a programů jak rozluštit/prolomit bezpečnost tajného klíče/WEPU. Například program AirSnort nebo WEPCrack používají slabinu WEP šifrování popsanou mimo jiné i spoluautorem šifry RC4 Adi Shamirem.

Závěrem je nutno dodat, že přes veškeré slabiny WEPu je používání tohoto mechanismu nejmenší nutnou ochranou bezpečnosti sítě před neautorizovaným vstupem. K nabourání se

do sítě chráněné tímto protokolem je zapotřebí trocha umu a v případě některých útoků i velkou dávku času. Například pomocí programu AirSnort, kdy je nutné zachytit velké množství dat - zhruba 5 - 6 milionu paketů. Aktivací WEPu dáváme přinejmenším najevo: „Toto je soukromá síť- nevstupovat!“.

6.1.2 WPA

Ještě před vydáním standardu 802.11i (řešící bezpečnostní otázky), bylo nutné uvést nějaké přechodné řešení. Tímto řešením se stalo WPA (což je vlastně podmnožina 802.11i), která obsahuje nové šifrování (TKIP) a řízení přístupu (802.1x). Důležitou vlastností protokolu WPA je, že ho lze použít jen v sítích s infrastrukturou (nikoli v ad-hoc).

Vyřešené slabiny WEPu pomocí TKIP a 802.1x :

- Není možné použít stejný inicializační vektor.
- Jsou ošetřeny tzv. „slabé klíče“.
- Přidána správa klíčů.
- Zlepšení systému autentizace a deautentizace.

Temporal Key Integrity Protocol - TKIP:

TKIP vylepšuje šifrovací mechanismus, pomocí kterého dochází k časté změně tajných klíčů. Dále je vylepšena kontrola integrity pomocí tzv. MIC (Message Integrity Code). Před startem šifrovacího procesu jsou k dispozici dva klíče: Dočasný klíč (128b) a klíč pro kontrolu integrity (64b). Před vstupem do mechanismu WEP se XORují hodnoty dočasného klíče a MAC adresy odesílatele. Výsledek se dále XORuje se sekvenčním číslem a předává se do WEPu (rozdělení výsledku na IV a klíč). MIC klíč, MAC adresy odesílatele a příjemce plus nešifrovaná zpráva vstupují do MIC algoritmu. Výstupem je 6 bajtů dlouhá sekvence připojovaná k přenášeným datům. TKIP zvětšuje bezpečnost zvýšením velikosti inicializačního vektoru na 48 bitů, dále určuje hodnotu IV tak, že se postupně zvětšuje od nuly do maximální hodnoty.

802.1x (někdy také **EAPOL** tedy Extensible Authentication Protocol (EAP) over LANs)

802.1x je protokol zajišťující větší kontrolu (bezpečnost) nad autentizačním a deautentizačním cyklem. V podstatě pracuje tak, že blokuje přístupové porty (na fyzické vrstvě) dokud se klient neprokáže. Záznamy o klientech jsou spravovány ve vzdálených serverech, většinou na RADIUS (Remote Authentication Dial In User Service) serveru, který je mimochodem implementován i ve Windows 2000. 802.1x využívá EAP (Extensible Authentication Protocol), což je ověřovací systém umožňující snadnou práci s hesly, tokeny i PKI (Public Key Infrastructure) certifikáty. Zajišťuje otevřený transportní mechanismus. V procesu autentizace se vyskytují 3 subjekty. **Žadatel** (supplicant -klient), **autentizátor** (většinou access point) a **autentizační server** (skladující informace o žadatelích). Ověřování probíhá tak, že v první řadě supplicant vyšle požadavek na autentizaci k autentizátoru. Autentizátor se pak dotáže na totožnost klienta (EAP-Request/Identity) a ten mu odpoví příslušnými údaji. Autentizátor se dotáže autentizačního serveru (předělá dotaz z EAP do RADIUS protokolu), zda údaje souhlasí s databází. Autentizační server se dotáže přes autentizátora klienta na jeho jméno a heslo (ten provede příslušnou transformaci těchto údajů a pošle je zpět). Server v případě souhlasu údajů odpoví a autentizátor povolí přístup klienta do sítě. Tento postup však nemusí být vždy stejný, je možné i jiná volba například při vzájemném (dvousměrném) ověřování je průběh mnohem komplikovanější.

802.1x umožňuje také několik bezpečnostních „vymožeností“, například lze definovat časovou prodlevu po které se musí supplicant znovu přihlašovat.

Ověřovací metody používané nad 802.1x:

EAP - MD5:

- jednocestná metoda používající k ověřování jméno a heslo. Je nejjednodušeji implementovatelná. Bohužel je také nejméně bezpečná (hesla jsou uložena v čitelné formě), nepodporuje dynamické generování WEP/TKIP klíčů.

EAP-TLS (Transport Layer Security):

- nejbezpečnější, ale také nejvíce komplikovaná na zavedení. Umožňuje obousměrnou autentizaci.

EAP-TTLS (Tunneled Transport Layer Security):

- vytvořením TLS spojení mezi autentizátorem a autentizačním serverem a libovolného spojení (například MD5) mezi autentizátorem a klientem zvyšuje jednoduchost implementace. Podporuje vzájemnou autentizaci i dynamické obnovování WEP klíčů.

Pro vytvoření zabezpečeného spojení s použitím 802.1x a příslušné EAP metody je nutné, aby byli tyto postupy podporovány ve všech třech účastnících ověřovacího procesu.

6.1.3 Standard 802.11i

Tento standard obsahuje již výše zmíněné komponenty TKIP, EAP s použitím 802.1x. Co však ve WPA nebylo zahrnuto byla šifra AES (Advanced Encryption Standard). Tato šifra se v 802.11i používá v čítačovém režimu s protokolem AES-CCMP (Counter Mode/ CBC-MAC Protocol), zajišťujícím autentizaci a integritu dat. Narozdíl od RC4, což je proudová šifra, je AES šifra bloková. Ta totiž pracuje s bloky dat o délce 128 bitů. Podstatou blokového šifrování se stává AES více náročná na hardwarový výkon, a tak je možná implementace pouze do nových zařízení.

Závěrem uvádím přehled dostupného zabezpečení:

Tabulka 3: Přehled dostupných možností zabezpečení

Zabezpečení	Šifrování	Autentizace
WEP	WEP	nepoužívá
WPA	TKIP	PSK
802.11i	AES	PSK
WPA	TKIP	802.1x
802.11i	AES	802.1x

Závěrem této kapitoly, však dodávám, že světové špičky na bezdrátovou technologii a její zabezpečení tvrdí, že používat bezdrátový přenos pro citlivá firemní data je na pokraji hazardu. Nabádají k tomu aby se hledaly možnosti drátového přenosu dat.

II. PRAKTICKÁ ČÁST

7 SOUČASNÝ STAV BEZDRÁTOVÝCH SÍTÍ WI-FI NA U5

Mobilní přístup do sítě internet se v posledních letech začínal prosazovat i v akademických prostorech. V současné době má většina univerzit v ČR možnost bezdrátového připojení. Nicméně na naší univerzitě do nedávné doby tento přístup nebyl možný. Před krátkou dobou se sice umožnil bezdrátový přístup v budově U1, bohužel však na reprezentativní budově fakulty technologické tato možnost stále chybí.

O bezdrátové síti v budově U5 můžeme hovořit pouze v rozmezí proprietárních řešeních jednotlivců. Ty jsou často realizovány bez vědomí odpovědných pracovníků UTB. Je nutno podotknout, že soukromé bezdrátové sítě se mohou podílet na rušení plánované oficiální sítě. V případné síti poskytující univerzitní internet může dojít k bezpečnostním rizikům z hlediska nezodpovědného zabezpečení. Veškerou neoficiální, neautorizovanou komunikaci na bezdrátové úrovni navrhuji, z bezpečnostního hlediska a kvalitativního hlediska pro budoucí bezdrátovou síť, omezit případně zrušit.

8 NÁVRH BEZDRÁTOVÉ SÍTĚ V AREÁLU UTB U5

V následující kapitole uvedu několik variant hardwarového a bezpečnostního uspořádání bezdrátové sítě. Bezpečnost je podle mě nejdůležitějším faktorem pro utváření bezdrátového pokrytí (a následné konektivity do internetu) areálů akademických sítí. Proto budu vždy při návrhu hardwarového vybavení sítě vycházet z vytvořené varianty zabezpečení.

8.1 Zabezpečení

Současné možnosti zabezpečení Wi-Fi (případně Wi-Fi5) sítí je poměrně na vysoké úrovni. Bohužel však při návrhu bezdrátové sítě na naší fakultě je nutno počítat s klienty, kteří nové standardy ve svých zařízeních implementovány nemají. Proto je nutno vytvořit bezpečnostní politiku na takové úrovni, aby konektivita do internetu nebyla pouze pro několik vyvolených, ale pro všechny studenty. Nicméně pro přehlednost navrhu i variantu nepočítající s hardwarovými nedostatky klientských zařízení.

8.1.1 Varianta 1: Bezpečnost na základě WEP

Dosažení minimální bezpečnosti je možno pomocí šifrovacího protokolu WEP, kdy by si klienti přihlašovaní do sítě museli nejprve zjistit tajný klíč od správce. Rozhodně tento klíč nedoporučuji publikovat na internetu, jako je to v případě bezdrátové konektivity na budově U1 fakulty technologické. Je sice pravda, že je tam použita i filtrace klientů pomocí tabulky MAC adres, nicméně existují programy, které tyto adresy dokáží změnit. Nabourání se do takové sítě je potom jen otázka zachycení MAC adresy v komunikaci a následné vyčkání na její uvolnění (jakmile se přihlášený student odpojí) a převzetí identity. Na druhou stranu je zavedení kontroly klientů na základě jejich MAC adres další překážkou, kterou je možno použít pro případné odrazení infiltrátorů. Pro WEP je dobré použít šifrovací klíč tím způsobem, že ho zadáme přímo hexadecimálně - nebudeme ho generovat z textu. Navrhuji volbu délky klíče na 104 bitů (kvůli kompatibilitě se staršími zařízeními). Velmi důležitou součástí bezpečnosti je také změna implicitních hesel na access pointech. S předpokladem použití více access pointů bude velmi praktické zavedení správy kontroly MAC adres pomocí RADIUS serveru.

Shrnutí varianty:

- WEP, 104 bitů, HEX klíč,
- kontrola klientů pomocí MAC adres ve spolupráci s RADIUS serverem.

Tato varianta nenabízí moc velkou úroveň bezpečnosti, ale na druhou stranu je dostupná pro všechny klienty a je jednoduše implementovatelná. V kombinaci s častou změnou WEP klíčů může být i s určitou mírou tolerance dostačující.

8.1.2 Varianta 2: 802.11i

Zabezpečení na nejvyšší možné úrovni by bylo možné dosáhnout použitím bezpečnostních protokolů v protokolu 802.11i. V dnešní době se nové zařízení prodávají s podporou 802.11i. Lze předpokládat, že s postupem času bude přibývat klientů, kteří tuto podporu budou ve svých klientských zařízeních mít. Šifrování pomocí AES zajišťuje mnohonásobně lepší bezpečnost než by byla dostupná ve variantě 1. Pro zřízení této varianty je nutné zavést do infrastruktury RADIUS server, který se ve spolupráci s 802.1x zajistí i autentizaci uživatelů na základě údajů na RADIUS serveru. Toho je možno docílit pomocí autentifikace EAP-TLS (jedna z mnoha variant v 802.1x).

Shrnutí varianty:

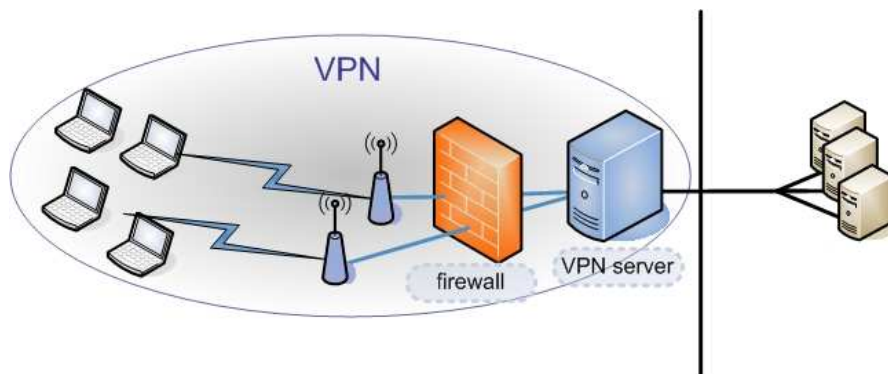
- WPA s šifrou AES
- autentizace pomocí EAP-TLS (802.1x)

Varianta nabízí nejlepší dostupné zabezpečení, nicméně by většina studentů UTB, vzhledem k zastaralosti svých klientských zařízení, nemohla k síti přistupovat. Časem by se zřejmě tato situace jistě zlepšila (s postupným dokupováním nových zařízení).

8.1.3 Varianta 3: VPN

Implementace VPN sítí jako bezpečnostní bariery se v akademických bezdrátových sítích uplatňuje poměrně často. Běžně se používají VPN tunely na přemostění spoje uživatel -

firemní síť, kdy za nedůvěryhodnou část přenosu je považován internet. Tato architektura lze využít i v našem případě, kdy za nedůvěryhodnou část budeme považovat bezdrátový přenos. Bude nutné vytvořit takovou architekturu, která by vynutila (pomocí firewallu umístěného bezprostředně za access pointy) přístup do internetu pouze přes VPN server.



Obrázek 23: Architektura VPN sítě

Jako tunelovací protokol bude nejlépe vyhovovat PPTP, který je podporován prakticky ve všech operačních systémech MS Windows (narozdíl od IPSec).

Server:

- operační systému Linux
- VPN server Poptop (http://www.linuxsoft.cz/sw_detail.php?id_item=617)
- RADIUS server FreeRadius (<http://www.freeradius.org/>)
- adresářová struktura LDAP (například OpenLDAP)

Nastavení serveru této konfigurace je předmětem bakalářské práce Jakuba Sporka.

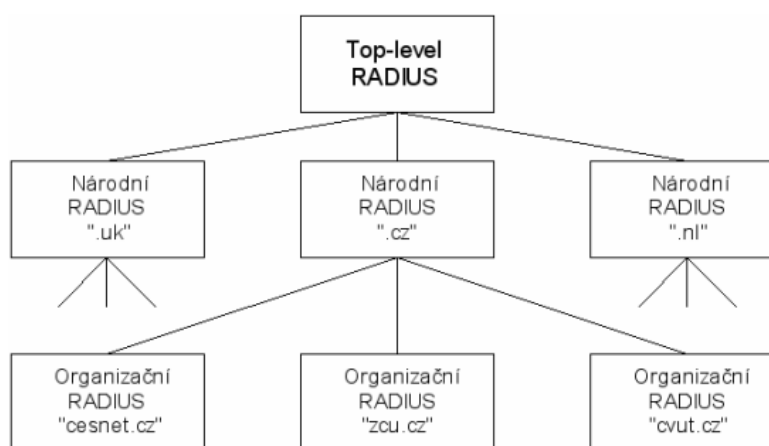
Pro verzi pod systémem MS Windows 2000 je možno provozovat server s prostředky implementovanými již v systému. Kompletní konfiguraci serveru pod systémem Windows 2000 je možno nalézt v knize [1]

Klienti si vytvoří účet a pomocí nástrojů pro napojení na VPN síť ve Windows se připojí k síti.

Tato metoda zabezpečení a přístupu do wi-fi sítě je poměrně bezpečná. Využívají ji i některé vysoké školy (Masarykova univerzita). Osobně ji vidím jako nejlepší možnou variantu.

8.1.4 Varianta 4: Systém EDUROAM

Další možností by bylo zapojit naši školu do systému eduroam (www.eduroam.cz) firmy CESNET. Systém slučuje databáze uživatelských účtů na všech zapojených školách do jedné stromové architektury. Jednotlivé RADIUS servery jsou mezi sebou propojeny IPSec tunely. Uživatelé se potom přihlašují ve tvaru `novak@utb.cz`, podle něhož se z navštíveného RADIUS serveru postupně dojde na domácí RADIUS server uživatele.



Obrázek 24: Struktura RADIUS serveru sítě EDUROAM

Tato varianta podporuje dvě rozhraní pro autentizaci uživatelů. První varianta je pomocí autentizace přes 802.1x a druhá přes www rozhraní (pro klienty bez podpory 802.1x). Souběžného běhu těchto rozhraní je docíleno pomocí dvou VLAN. Proto je zapotřebí access pointy podporující separátní VLAN.

Zapojení se do systému eduroam je umožněno po zajištění několika požadavků. Například vyžadují administrátora, který „bude schopen do jednoho pracovního dne zareagovat na požadavky správců národních RADIUS serverů tak, aby nebyla nijak ohrožena funkce žádné části infrastruktury.“ Veškeré požadavky je možno případně dohledat na internetové adrese: [6]

8.2 Hardware

Při volbě hardwaru je nutné brát zřetel na zamýšlené zabezpečení. Proto při volbě navrhovaných variant byly hodnoceny právě ty parametry, které při zabezpečení hrají roli. Dalšími důležitými parametry jsou například: možnost regulace a hodnota výstupního výkonu.

Access pointy:

ASUS WL-500G

Technické parametry:

Standardy: 802.11b, 802.11g

Management: WEB

Šifrování: TKIP, AES, WPA, WPA-PSK

Ověřování: MAC adresy, 802.1x

Konektory: RJ45, USB, D-SUB (tiskárna), WAN

Anténa: interní a dipólová externí (reverzní SMA konektor)

Výstupní výkon: 12 - 15 dBm

- podpora VPN průchodu (PPTP, L2TP, IPSec)

Orientační cena: zhruba 2 700,- Kč bez DPH

Toto zařízení vyhovuje prvním třem variantám zabezpečení, nemá však podporu separátních VLAN, takže ho nelze nasadit ve variantě zapojující se do systému eduroam. Vyhovuje však ostatním variantám (1-3). Umožňuje připojení USB zařízení. Bylo by jistě zajímavé nabízet, za pomoci IP kamery, na stránkách UTB živý obraz reprezentativního atrie U5.

Cisco AIR-AP1121G-E-K9

Technické parametry:

Standardy: 802.11b, 802.11g

Management: konzola (CLI), Telnet, web mgmt (GUI), SNMP, FTP a TFTP

Zabezpečení: 802.11i

Anténa: externí se ziskem 2,2dBi

Další vlastnosti:

Vlastní operační systém. Nastavitelný vysílací výkon (do 100mW). Podpora vytváření až 16 VLAN dle 802.11q. Firmware AP připraven pro upgrade na QoS standard dle 802.11e, Load Balancing, Power over Ethernet napájení,...

Orientační cena: 11 000,- Kč bez DPH

Zařízení firmy CISCO jsou jedny z nejlepších, ne-li nejlepší co je možno pořídit ve světě wireless. Tento access point poskytuje velmi výkonnou složku případné sítě. Je například využíván i v bezdrátové síti Univerzity Karlovy. Bohužel bohatou výbavu také reflektuje cena tohoto zařízení. Toto zařízení vyhovuje samozřejmě pro všechny varianty (včetně systému eduroam).

Antény:

Použitím antény u access pointů lze docílit několika věcí. Rozšíří se dostupnost signálu, který je díky externím anténám lépe směrovatelný. Tím je možno docílit pokrytí pouze tam, kde je to třeba. Sníží se tím riziko infiltrace. Zesílením signálu, však naroste i velikost rušení. Nicméně použití antén je výhodné. Volba bude závislá přímo na umístění, které je závislé na charakteristice pokrývaného prostředí (jeho nehomogenitě v různých směrech). Například sektorová anténa D-Link Indoor antenna (zisk 6dBi) by byla vhodná k pokrytí atri U5.

Server:

Jako server lze využít některého již zakoupeného počítače. Například při nasazení varianty s Linuxovým serverem není zapotřebí přílišného výkonu. Proto bude možné využít některého již téměř vyřazeného počítače. V případě zakoupení nového stroje, postačí PC v cenové relaci 12 000,- Kč bez DPH.

8.3 Rozmístění a počet access pointů

Instalace bezdrátových zařízení bývá většinou realizován firmami zabývajícími se touto činností. Navrhnutí pokrytí signálu uvnitř budov je často považováno za prakticky nemožné. Do hry totiž vstupují charakteristiky jako je propustnost zdí, nebo nárůst rušení vlivem zapojení více access pointů. Na alespoň odhad propustnosti jsem provedl měření, jež bude popsán v následující kapitole. Na závěr bude navrhnout přibližný počet a umístění access pointů.

8.3.1 Měření propustnosti signálu v lokalitě U5

Použité nástroje

Access point:

D-Link DWL 2100 - Vysílací výkon: 15dBm (32mW) $\pm$ 2dB, Anténa: 1,0 dB

Klient:

Notebook s operačním systémem Windows XP a USB stick ASUS (802.11g)

Program NetStumbler:

Nástroj na zjišťování kvality signálu popřípadě detekci sítí. Program graficky znázorňuje průběh kvality signálu, kde se červeně vyobrazuje hladina šumu (noise) a zeleně úroveň signálu (signal). Vyobrazení je v jednotkách dBm (výkon vyjádřený relativně, vztažený k výkonu 1mW). Průběh signálu jde sumarizovat a exportovat do textového souboru, kde lze vyčíst hodnota SNR (odstup signálu od šumu).

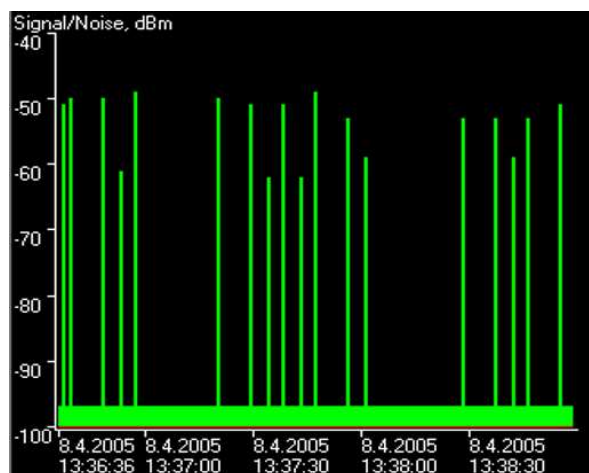
Vztah pro přepočet výkonu (P) ve W na výkon v dBm:

$$\text{dBm} = 10 * \log_{10}(P / 0.001) \quad (4)$$

Měření

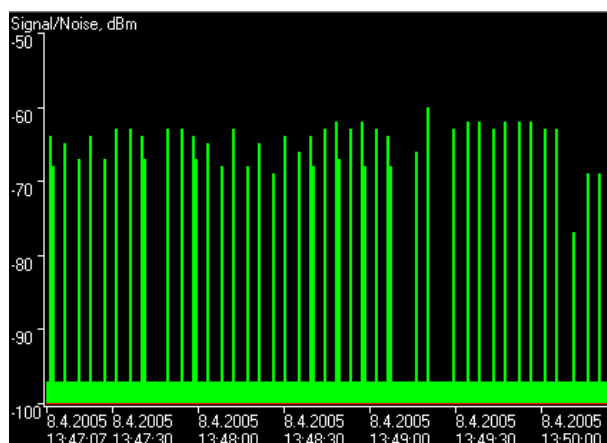
Při měření byl access point nastaven do modu infrastructure bez šifrování, SSID na hodnotu D308 a byl použit kanál 6. Access point byl umístěn v počítačové místnosti číslo 204.

Úroveň signálu v místnosti s access pointem byla na vysoké úrovni. SNR byl 83 dBm. Při přesunu notebooku do vedlejší místnosti došlo k degradaci kvality signálu na hodnotu SNR 51 dBm.



Obrázek 25: Průběh signálu ve vedlejší místnosti

Úroveň SNR v místech, kam se signál musel dostat přes 2 příčky, poklesla na hodnotu 40 dBm, tato hodnota je považována za celkem uspokojivou. Nicméně bude dobré ji považovat jako poslední možnou.



Obrázek 26: Průběh signálu průchozího přes 2 příčky

Signál procházející třemi příčkami byl na tak nekvalitní úrovni (SNR 24 dBm), že docházelo k výpadkům spojení. Vzhledem k tomu, že nebyly v lokalitě zapojeny jiné

access pointy a nedocházelo tak k vzniku rušení je tato hodnota brána jako naprosto neuspokojivá.

Bylo provedeno několik měření i v dolním patře, tam bohužel signál přes strop neprostupoval, což mohly způsobit železné části stropu, nebo špatně natočená anténa (všesměrová anténa - malý vertikální úhel - pokrytí pod anténou je malé).

Vyhodnocení:

Průchodnost signálu ukazuje následující tabulka.

Tabulka 4: Hodnocení průchodnosti signálu

Počet příček	SNR [dBm]	Hodnocení
0	83	výborné
1	51	dobré
2	40	dostačující
3	24	nedostačující

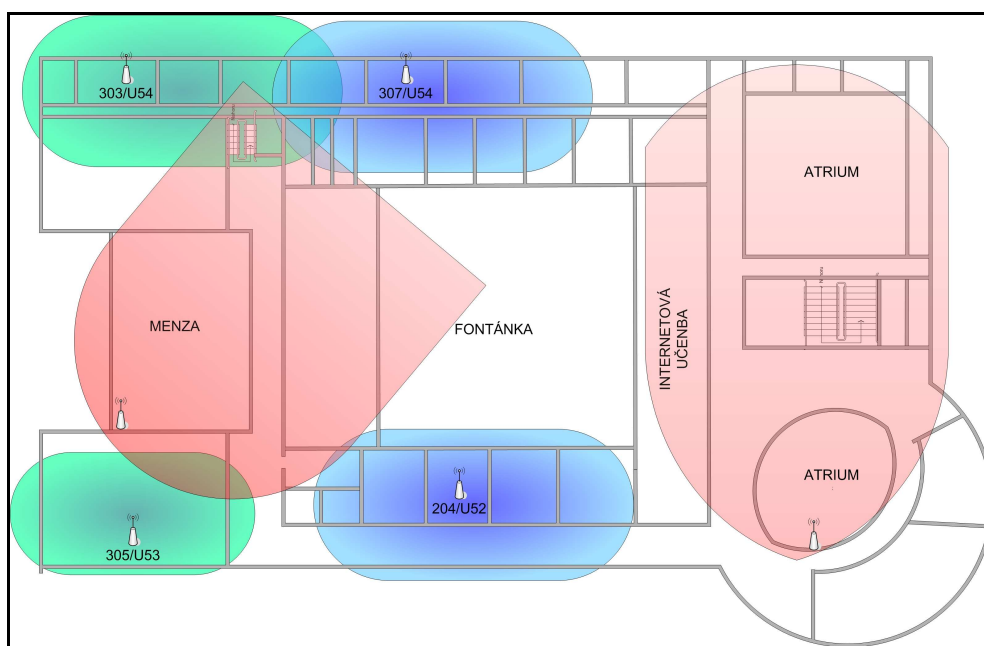
8.3.2 Návrh rozmístění access pointů

Z měření zdí na propustnost signálu je patrné, že při použití AP bez externí antény dochází k poklesu na kritickou mez po třech příčkách, přes vnější zdivo po dvou a u stropů nedochází k průchodu prakticky vůbec. Na to je tedy nutné brát zřetel.

Tabulka 5: Umístění access pointů

Access point	Umístění
1.	Atrium
2.	204/U52
3.	108/U52
4.	Menza
5.	307/U54
6.	108/U54
7.	303/U54
8.	305/U53

Rozmístění přístupových bodů ukazuje následující obrázek, kdy jednotlivé barvy vyjadřují zvolený kanál (1,6,11). Podotýkám, že je zakresleno pouze 1. patro. Access pointy umístěné v přízemí nejsou tedy zobrazeny. Oba skryté AP jsou zhruba na stejné úrovni jako ty s modrou oblastí pokrytí (jsou pod nimi). V menze a atriu předpokládám použití sektorových antén, všude jinde navrhuji všesměrové. Access point v atriu bude výhodné umístit nad schodiště (tak, aby viděl do přízemí i do prvního patra).



Obrázek 27: Pohled na rozmístění access pointů

8.4 Cenová kalkulace

Cena bezdrátového pokrytí budovy U5 se bude lišit podle počtu použitých přístupových bodů, ale hlavně podle volby varianty zabezpečení. Pokud bychom zvolili variantu zapojení se do systému eduroam, tak podle mého návrhu access pointu (Cisco AIR-AP1121G-E-K9) bude pokrytí výrazně dražší, než při použití přístupového bodu ve variantách 1-3 (ap ASUS WL-500G).

Tabulka 6: Cenová kalkulace

	Varianta		Popis
	Cisco	Asus	
AP	88 000 Kč	21 600 Kč	8 access pointů
Antény	1 400 Kč	1 400 Kč	2 antény D-Link Indoor antenna
Server	12 000 Kč	12 000 Kč	Při využití již zakoupeného PC: 0,- Kč
Ostatní	3 000 Kč	3 000 Kč	Kabeláž, konektory...
Celkem	104 400 Kč	38 000 Kč	

Jak je vidět z tabulky je varianta s použitím access pointů od firmy Cisco zhruba o osmdesát tisíc dražší, než druhá varianta. Ovšem na druhou stranu dostaneme kvalitní access pointy s bohatou podporou od výrobce a rozličnými možnostmi využití. Ikdyby byla například zvolena varianta zabezpečení pomocí VPN tunelů, tak by byla síť připravena pro eventuelní přechod do systému eduroam.

V případě použití již zakoupeného PC na server se cena může snížit na 91 000,- Kč a 24 600,- Kč. Je nutné, však upozornit na fakt, že počet access pointů se může změnit v závislosti na konkrétní situaci. Kvůli tomu se mohou ceny obou variant podstatně změnit.

8.5 Porovnání navržených variant

V kapitole 8.1 byly navrženy čtyři varianty zabezpečení bezdrátové sítě.

První varianta je založena na použití protokolu WEP + kontrole MAC adres spravovaných pomocí RADIUS serveru. Tato možnost nabízí nejjednodušeji spravovatelný systém, nicméně také nejmenší úroveň zabezpečení.

Druhé řešení zabezpečení stávající se z využití nejnovějších bezpečnostních zásad stanovených ve standardu 802.11i. Varianta poskytuje nejvyšší možnou úroveň zabezpečení a srovnatelnou náročnost na správu jako první varianta. Nicméně již svou podstatou zamezuje použití u všech klientských zařízeních.

Vytvoření VPN tunelů je popsáno ve variantě 3. Bezpečnostní úroveň této varianty je plně dostačující. Celková implementace této varianty je složitější než předchozí dvě. Na správu je poté nutné vynaložit větší úsilí, jež však ale zajišťuje dostatečnou bezpečnostní úroveň a podporu pro všechny klientské zařízení.

Poslední variantou je zapojení se do roamingového systému eduroam firmy CESNET. Z hlediska provozní náročnosti je pravděpodobně tou nejnáročnější variantou. Jsou požadovány odpovědné osoby, jež budou schopny do určité časové doby zajistit obnovu provozu v případě poruchy. Správce by měl mít také právní vztah k firmě Cesnet. Na druhou stranu však poskytuje nejvyšší možnou míru zabezpečení s ohledem na možnosti klientských zařízení.

Jako nejvíce vyhovující se zdá VPN zabezpečení (tedy varianta číslo 3). Toto řešení je již provedeno i na ostatních univerzitách a poskytuje dostačující bezpečnostní úroveň. Při zavedení tohoto přístupu, lze využít server vytvořený Jakubem Sporkem v jeho letošní bakalářské práci.

Cenová náročnost výstavby bezdrátové sítě na U5 je závislá na volbě hardwarového vybavení. Byly navrženy dvě varianty. Jedna poskytuje podporu jen pro první tři varianty a druhá nabízí možnost zapojení se i do systému eduroam. První varianta řešená přístupovými body Asus WL-500g vyjde zhruba na 40 000,- Kč. Možnost zapojení se do systému eduroam, však vyžaduje náročnější hardware. Cena této varianty se poté vyšplhá na něco přes 100 000,- Kč. Osobně však doporučuji vzhledem k budoucí perspektivě volbu druhé dražší varianty.

ZÁVĚR

Hlavním cílem této práce bylo navrhnout několik variant umožnění bezdrátové konektivity do internetu v areálu UTB U5. Významným kritériem poskytování internetu na bezdrátové úrovni je zajištění co možná největší míry zabezpečení s ohledem na hardwarové možnosti klientských zařízení. To bylo zohledněno a vypracováno několik variant zabezpečení, z nichž nejperspektivnější se jeví vytvoření VPN tunelů s využitím protokolu PPTP. Je však nutné konstatovat, že vytvoření naprosto bezpečné bezdrátové sítě je neuskutečnitelné.

Hardwarové řešení sítě je možno realizovat pomocí dvou navržených variant, které se liší typem použitých přístupových bodů. Pokrytí vytipovaných míst je uskutečnitelné v cenových relacích 40 a 110 tisíc Kč, v závislosti na volbě hardwarové varianty. Jako nejperspektivnější řešení se jeví druhá varianta využívající bezdrátové přístupové body firmy Cisco. Toto finančně náročnější řešení, však do budoucna poskytuje dostatečnou míru flexibility. Je tedy možné se v případě zájmu zapojit i do roamingového systému firmy CESNET, ve kterém je již v současné době zapojeno několik vysokých škol nejen z České republiky.

Poskytování bezdrátové internetové konektivity v akademických sítích se v posledních letech stává již standardní záležitostí. Lze předpokládat, že k tomuto trendu dojde i v areálech středních a základních škol. Budoucnost bezdrátových sítí (jako takových) je zatím nejasná, nicméně lze usuzovat, že dojde k nárůstu rychlosti přenosu na srovnatelnou úroveň s metalickou kabeláží. Svoji „nebezpečností“ si nejspíše nevybudují postavení ve firemních sítích, ale s velkou pravděpodobností dojde k masivnímu rozšíření tzv. hotspotů, kdy je možné buď za poplatek nebo zdarma se bezdrátově připojit k internetu. Rozšiřování bezdrátových sítí bude, však zcela jistě narážet na bariéry vzniklé vzájemným rušením.

SEZNAM POUŽITÉ LITERATURY

- [1] BARKEN, Lee. *Jak zabezpečit bezdrátovou síť Wi-Fi*. 1. vyd. Brno : Computer Press, 2004. ISBN 80-251-0346-3.
- [2] KÖHRE, Thomas. *Stavíme si bezdrátovou síť Wi-fi*. 1. vyd. Brno : Computer Press, 2004. ISBN 80-251-0391-9.
- [3] ZANDL, Patrick. *WiFi Praktický průvodce*. Brno : Computer Press, 2003. ISBN 80-7226-632-2.
- [4] PUŽMANOVÁ, Rita. *Širokopásmový Internet - Přístupové a domácí sítě*. Brno: Computer Press, 2004. ISBN 80-251-0139-8.
- [5] *Webblog P. Zandla - WiFi* [online]. Dostupný z WWW: <<http://www.marigold.cz>>.
- [6] *Projekt eduroam fy CESNET* [online].
Dostupný z WWW: < <http://www.eduroam.cz> >.
- [7] *Web o bezdrátových technologiích* [online].
Dostupný z WWW: <<http://www.wifionline.net>>.
- [8] *WiFi sekce serveru Lupa.cz* [online]. Dostupný z WWW: < <http://wifi.lupa.cz/>>.
- [9] *Server věnovaný počítačovým sítím* [online].
Dostupný z WWW: < <http://www.svetsiti.cz/>>.
- [10] *Český telekomunikační úřad* [online]. Dostupný z WWW: <<http://www.ctu.cz>>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Ad-hoc	Typ architektury bezdrátových sítí bez access pointu
AES	Advanced Encryption Standard - bloková šifra použitá v 802.11i
AP	Access Point - přístupový bod
BSS	Basic Service Set - jednoduchá Wi-Fi síť s jedním access pointem
CCK	Complementary Code Keying - doplňkové kódové klíčování
CRC	Cyclic Redundancy Check - kontrolní součet
ČTÚ	Český Telekomunikační Úřad
DCF	Distributed Coordination Function - režim přístupu k médiu
DSSS	Direct Sequence Spread Spectrum - metoda přenosu dat
EAP	Extensible Authentication Protocol -rozšiřitelný ověřovací protokol
EDCF	Enhanced Distribution Coordination Function - rozšířený režim DCF o QoS
ESS	Extended Service Set - několik sítí typu BSS
FHSS	Frequency Hopping Spread Spectrum - druh frekvenční modulace
FTP	File Transfer Protocol - protokol pro přenášení souborů
HCF	Hybrid Coordination Function - rozšíření PCF ve standardu 802.11e (QoS)
IAPP	Inter Access Point Protocol - protokol zajišťující roaming na 2. OSI vrstvě
IBSS	Independent Basic Service Set - jiný název pro ad-hoc síť
IEEE	Institute of Electrical and Electronics Engineers - standardizační instituce
IPSec	IP Security protocol - bezpečnostní protokol
IT	Information Technologies
IV	Inicializační vektor - vektor používaný ve WEP šifrování
L2TP	Layer 2 Tunnel Protocol - bezpečnostní protokol
MAC	Media Access Control - podvrstva 2. vrstvy OSI

MIC	Message Integrity Code - kód pro kontrolu integrity
OFDM	Orthogonal Frequency-Division Multiplexing - metoda frekvenční modulace
OSI	Open System Interconnect - model síťové hierarchie
PCF	Point Coordination Function - režim přístupu k médiu
PoE	Power over Ethernet - napájení po nevyužívaných drátech ethernetu
PPTP	Point-Point Tunneling Protocol - bezpečnostní protokol
QoS	Quality of Service - kvalita služeb (802.11q)
QPSK	Quadrature Phase Shift Keying - typ modulace
RADIUS	Remote Authentication Dial In User Service - server pro ověřování identity
RC4	Proudová šifra používaná ve WEP
RTS/CTS	Request-To-Send/ Clear-To-Send - mechanismus přístupu k médiu
SNR	Signal-to-Noise Ratio Odstup signálu od šumu
SSID	Service Set Identifier - řetězec označující Wi-Fi síť
TKIP	Temporal Key Integrity Protocol - šifrovací protokol s dynam. změnou klíče
TLS	Transport Layer Security - autentizační metoda protokolu EAP
TTLS	Tunneled Transport Layer Security - autentizační metoda protokolu EAP
VPN	Virtual Private Network - virtuální privátní síť
WDS	Wireless Distribution System - systém bezdrát. propojení přístupových bodů
WEP	Wired Equivalent Privacy - bezpečnostní mechanismus
Wi-Fi	Wireless Fidelity - bezdrátové síť na frekvenci 2,4 GHz
Wi-Fi5	Wireless Fidelity - bezdrátové síť na frekvenci 5,8 GHz
WLAN	Wireless Local Area Network - bezdrátová síť
WPA	Wi-Fi Protected Access - bezpečnostní mechanismus
XOR	Nonekvivalence

SEZNAM OBRÁZKŮ

Obrázek 1: Schéma roamingu	16
Obrázek 2: Access point fy D-Link	20
Obrázek 3: Asus 500g -router, ap, switch,.....	21
Obrázek 4: PCI adaptér	22
Obrázek 5: USB stick	22
Obrázek 6: PCIMCIA karta	23
Obrázek 7: SD wireless card.....	24
Obrázek 8: Směrová yagi anténa	25
Obrázek 9: Sektorová anténa	25
Obrázek 10: Všesměrová anténa.....	26
Obrázek 11: N female, krimpovací konektor.....	29
Obrázek 12: RSMA Female a Male konektor.....	29
Obrázek 13: Female a Male konektor Lucent.....	30
Obrázek 14: Pigtail	30
Obrázek 15: PoE pro AP Ovis 1120	31
Obrázek 16: Ad-hoc síť	34
Obrázek 17: BSS/ESS síť	35
Obrázek 18: Point to multipoint architektura	35
Obrázek 19: Struktura sítě s repeaterem	36
Obrázek 20: Ukázka WDS sítě	36
Obrázek 21: Fresnelova zóna.....	37
Obrázek 22: Princip WEP šifrování.....	41
Obrázek 23: Architektura VPN sítě	50
Obrázek 24: Struktura RADIUS serveru sítě EDUROAM.....	51
Obrázek 25: Průběh signálu ve vedlejší místnosti	55
Obrázek 26: Průběh signálu průchozího přes 2 příčky	55
Obrázek 27: Pohled na rozmístění access pointů.....	57

SEZNAM TABULEK

Tabulka 1: Rozdělení frekvencí v radiových sítích	10
Tabulka 2: Orientační ceny	33
Tabulka 3: Přehled dostupných možností zabezpečení	44
Tabulka 4: Hodnocení průchodnosti signálu	56
Tabulka 5: Umístění access pointů	56
Tabulka 6: Cenová kalkulace.....	58