

**JIHOČESKÁ UNIVERZITA**  
**PEDAGOGICKÁ FAKULTA**  
**KATEDRA INFORMATIKY**

**Realizace školní bezdrátové sítě**

Petr Syrovátka

Vedoucí diplomové práce: PhDr. Milan Novák, Ph. D.

České Budějovice 2012

## Anotace

Diplomová práce se zabývá v teoretické rovině výzkumem současného stavu školské infrastruktury a požadavků na její doplnění o prvky bezdrátových technologií. Zkoumá požadavky a specifické situace, které jsou charakteristické pro školské prostředí a odlišují jej od běžných komerčních aplikací. Dále se zabývá vlivem nastupujícího trendu masového rozšíření informačních a komunikačních prostředků využívajících bezdrátové technologie na pedagogy a studenty. V praktické části práce je tvořen návrh modelového řešení pokrytí školní budovy bezdrátovou sítí. Jsou zde rozebírány nejen technické požadavky na použité komponenty, ale i rozbor dostupných technologií vyskytujících se na trhu. Práce řeší i problematiku projekce a návrhu bezdrátové sítě, měření a vlastností signálu šířeného v budovách. Vzniká tak jakýsi návod na realizaci jednoho z možných technologických řešení s ohledem na specifika školského prostředí.

The diploma thesis deals with the theoretical research of the current state of educational infrastructure and requirements for its complementarity with the elements of wireless technologies. It looks into the requirements and specific situations typical for school environments and differs them from common commercial applications. It also deals with the influence of the incoming trend of mass spreading of informational and communicational means using wireless technologies among educators and also students. In the practical part of the work a design of model arrangement for wireless network coverage of a school building is created. Not only technical requirements for used components are analysed here, but also the available technologies on the market. The thesis also deals with the projection and designing a wireless network issues, but also the qualities and measuring of the wireless coverage in buildings. There arise instructions for the realisation of one of the possible technological arrangements concerning the particularities of a school environment.

## Prohlášení

Prohlašuji, že svoji diplomovou práci jsem vypracoval/a samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své diplomové práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích 11. 4. 2012

Petr Syrovátka

# OBSAH

<b>1. ÚVOD</b> .....	<b>8</b>
<b>2. CÍLE DIPLOMOVÉ PRÁCE</b> .....	<b>10</b>
<b>3. INFORMAČNÍ TECHNOLOGIE VE ŠKOLSKÉM PROSTŘEDÍ</b> .....	<b>10</b>
3.1. Přístup žáků k bezdrátovým technologiím.....	11
3.2. Možnosti a rizika řízení bezdrátového přístupu k síti.....	13
3.2.1. Možnosti řízení přístupu k bezdrátové síti .....	14
3.2.2. Rizika přístupu k bezdrátové síti.....	15
<b>4. VÝZKUM SPECIFIK ŠKOLSKÉHO PROSTŘEDÍ</b> .....	<b>16</b>
4.1. Šetření .....	17
4.2. Výsledky šetření.....	18
4.3. Požadavky na řešení.....	21
<b>5. DOSTUPNÉ TECHNOLOGIE</b> .....	<b>22</b>
5.1. Rozbor dostupných technologií.....	22
5.1.1. 2.4GHz 54 Mbps Wireless SMC EliteConnect Hotspot Gateway .....	22
5.1.2. TekRADIUS server pro Windows .....	24
5.1.3. OS MikroTik a MikroTik Router Board .....	27
5.2. Výběr technologie.....	29
5.3. Platforma MikroTik.....	29
<b>6. REALIZACE</b> .....	<b>33</b>
6.1. Projekční zadání.....	33
3.1.1. Stávající infrastruktura - výchozí podmínky.....	33
6.1.1. Požadavky na projektové řešení.....	34
6.2. Projekce.....	35
6.3. Měření .....	41
6.3.1. Realizace měření .....	42
6.4. Frekvenční pásmo .....	46
6.5. Řízení provozu bezdrátové sítě .....	47
6.5.1. Neúnosné zatížení připojení k internetu.....	47
6.5.2. Přístup k nevhodnému obsahu .....	49
6.5.3. Neautorizovaný přístup.....	50
6.6. Konfigurace RouterBoardu Mikrotik .....	51
6.6.1. Prostředí WinBox.....	51

6.6.2.	Nahrání konfiguračního skriptu .....	52
6.6.3.	Personalizace nastavení síťových rozhraní .....	54
6.6.4.	Personalizace přihlašovací stránky HotSpotu .....	55
<b>6.7.</b>	<b>Bezdrátová infrastruktura.....</b>	<b>56</b>
<b>6.8.</b>	<b>Připojení bezdrátové části sítě.....</b>	<b>58</b>
<b>6.9.</b>	<b>Administrace uživatelů .....</b>	<b>60</b>
<b>6.10.</b>	<b>Rozpočet na realizaci modelového řešení.....</b>	<b>61</b>
<b>7.</b>	<b>ZÁVĚR .....</b>	<b>62</b>
<b>8.</b>	<b>LITERATURA .....</b>	<b>64</b>
<b>9.</b>	<b>PŘÍLOHY .....</b>	<b>65</b>
<b>9.1.</b>	<b>Průvodní dopis k dotazníkovému šetření .....</b>	<b>65</b>
<b>9.2.</b>	<b>Dotazník statistického šetření.....</b>	<b>66</b>
<b>9.3.</b>	<b>Pravidla užívání bezdrátové sítě Českého reálného gymnázia s. r. o. CRG_WiFi .....</b>	<b>67</b>
<b>6.4</b>	<b>Cenová kalkulace.....</b>	<b>68</b>

# 1. Úvod

Téma diplomové práce bylo stanoveno z na základě faktu, že se ve školském prostředí objevuje obrovská škála digitálních informačních a komunikačních technologií určených pro vzdělávací proces. Prezentační technologie ve třídách se stávají pomalu ale jistě běžnou součástí práce pedagoga. Počítač se stal vybavením, které pedagogovi nahrazuje stále častěji běžnou formu agendy, jako jsou třídní knihy, klasifikační archy a katalogy, ale představuje pro něj i prostředek, pomocí něž si vytváří přípravy a podklady do hodin, koncepty písemných prací, případně interaktivních cvičení pro použití přímo hodině. Pedagogická práce se samozřejmě sestává i v rovině nepřímé pracovní doby z tvorby příprav a podkladů pro výuku, která učitel nemusí nutně vytvářet na pracovišti, ale i doma.

Ze strany některých ředitelů i zřizovatelů vzniká požadavek, aby škola disponovala takovou infrastrukturou, která umožní pedagogům přístup ke školní agendě, aplikačnímu serveru, síťovým úložištím a samozřejmě k internetu pomocí bezdrátových technologií. Prakticky každá škola je vybavena připojením k internetu a podle velikosti školy i serverem a příslušným lokálním síťovým rozvodem. Kvalita, rozsah i koncepce IT infrastruktury se však velice liší. Práce se mimo jiné pokusí prokázat spojitost mezi dostupností připojení ke školní síti a internetu a využívání informačních technologií ve vzdělávacím procesu. V této části se budu také zabývat mírou použití těchto technologií v závislosti na tom, zda je umožněno učitelům připojit se do školní lokální sítě, potažmo do internetu, vlastní techniku, na kterou je zvyklý a se kterou pracuje v rámci vlastní přípravy například v domácím prostředí.

Zcela specifickou rovinou je poskytnutí připojení samotným žákům. Zde vzniká celá řada dalších otázek spojených s bezpečností, možnostmi infrastruktury, kvalitou připojení školy do internetu, ale také otázky organizační, etické a pedagogické. Nedá se předpokládat, že v této rovině nenastane obecná shoda a že každá škola bude preferovat svůj model a postoj ke zmíněné problematice vycházející z typu a prostředí školského zařízení, věku i převládající sociální skupině žáků, případně i lokality, ve které se škola nachází.

Nutně nezanedbatelným měřítkem pro dostupnost informačních technologií je i finanční náročnost souvisejících projektů. Omezené rozpočty a seškrtnané investiční prostředky nepostihují pouze sektor školství a nedá se předpokládat, že by se v dohledné době našel zázračný zdroj prostředků, který by pokryl požadavky spojené s obnovou a rozšířením informačních a komunikačních technologií do vzdělávacího procesu. Už jen samotná odpovědnost na specifikaci takové investiční akce je přenášena na ředitele škol, kteří ve spolupráci s ICT koordinátorem definují zadání. Takové zadání někdy bohužel postrádá ohledy na další nutné investice, které jsou nutné pro využitelnost požadovaných technologií. Vzniká tak stav, kdy se investované prostředky nedaří zcela využít a nenaplnují původní záměr.

Pro ilustraci lze uvést příklad, kdy škola požaduje nákup patnácti notebooků pro vytvoření tak zvané mobilní učebny. Takovou učebnu je možné zřídit do libovolné třídy ve škole a využít ji pro výuku i v neinformatických předmětech. Není tak vázaná na učebnu informační techniky, která je hojně využívána pro výuku kmenových předmětů. Náklady na takovou akci snadno odhadne i člověk průměrně se orientující na trhu s informačními technologiemi. Může se ovšem ostát, že bude přehlédnut fakt, že nakoupené počítače musí být při výuce připojeny do elektrické sítě, kterou je třeba alespoň v některých učebnách rozšířit. Dále je vhodným požadavkem, aby byly počítače připojeny do školní sítě a sdílely připojení k síti internet a to připojením, které neohrozí bezpečnost stávající infrastruktury. Musí se předpokládat, že stávající síť bude s novou technikou spolupracovat v rozsahu, na který byli uživatelé zvyklí. V neposlední řadě musí být technika mimo výuku patřičně uložena a bezpečně skladována. Takové podružné investice pak mohou dosáhnout výše, která původní předpokládanou částku podle rozsahu až zdvojnásobí. Takové uvažování ve školském prostředí může chybět a ze strany zřizovatelů, kteří by měli mít příslušný odborný a poradní aparát, je odpovědnost přenášena přímo na zřizovaná pracoviště, respektive jejich ředitele. Ti však nemusí být odborníky, kteří postihnou veškeré aspekty. Obecná metodika zde chybí a definice takových investičních akcí je řešena přes dodavatelské firmy, informatiky na školách, rodiče a známé. Vzniká tak určitá míra opatrnosti, která do značné míry zpomaluje integraci nových technologií ve školách, potažmo ve vzdělávacím procesu.

## 2. Cíle diplomové práce

V rámci diplomové práce byly stanoveny dva základní cíle:

- První cíl představuje základní teoretický výzkum, postihující vybavenost škol síťovými technologiemi s ohledem na vnitřní přístupnost k internetovému připojení a ostatním službám v rámci školní sítě. Zabývá se specifickými požadavky vyplývajícími z odlišností od běžných aplikací. Tato část se mimo jiné soustředí i na principy bezpečnosti, které jsou neméně důležitým aspektem, především v zohlednění požadavku na přístupnost ze strany žáků i pedagogů a jejich přístupu k síti.
- Druhým cílem je návrh samotné infrastruktury vnitřní sítě zohledňující všechny aspekty a technické požadavky vyplývající z provedené analýzy školského prostředí. Tento návrh bude realizován a bude ověřena jeho funkčnost na příkladu modelové školy. V praktické části tak, kromě popisu řešení, vznikne jakýsi návod pro případné zájemce o podobnou aplikaci.

## 3. Informační technologie ve školském prostředí

Používání výpočetní techniky nabývá masových rozměrů v celé společnosti, nevyjímaje pracovníky ve školství. Tomuto trendu napomáhá stále větší cenová dostupnost výpočetní techniky a rozšiřující se nabídka trhu. Stále více pedagogů si z vlastních zdrojů pořizují výpočetní techniku, kterou využívají nejen pro soukromé účely, ale i pro zkvalitnění a zvýšení efektivity vlastní pedagogické práce. Vzhledem ke sblížování cen přenosných počítačů a stabilních zařízení se uchyluje stále více uživatelů k nákupu notebooků, které využívá flexibilně v domácnosti i v zaměstnání. Spolu s využíváním mobilních technologií nastupuje i stále rozšiřující se použití bezdrátových připojení v rámci lokálních sítí. Uživatel si volně volí pracovní místo, není omezen klasickým datovým rozvodem a ve většině případů se dá tvrdit, že kvalita i rychlost připojení, alespoň v lokálních sítích, nejsou do značné míry omezeny zvoleným typem připojení. Nastupuje ale otázka zprostředkování připojení takovým uživatelům, bezpečnosti a stability sítě a samozřejmě omezením přístupu neautorizovaných uživatelů do lokálních sítí. Bezpečnostní rizika nacházíme i v souvislosti s ochranou integrovaných zařízení. Celá řada uživatelů podceňuje



antivirovou ochranu svých počítačů, bezpečnostní aktualizace svých operačních systémů i ochrany dat na svých počítačích. Na administrátorovi takové sítě je, aby eliminoval možná rizika na straně sítě i uživatelů a stanovil vhodný systém zabezpečení a přístupu k síťovým prostředkům. Je nutné předpokládat, že běžný uživatel bude očekávat jistý stupeň podpory sítě, do které se připojuje. Samotná konfigurace parametrů síťových připojení, které bude odlišné v jednotlivých sítích, kde se uživatel pohybuje, může být pro některé i průměrně erudované uživatele věcí mimo jejich rozlišovací schopnosti a bude tak zdrojem jejich neopodstatněných stížností a mnoha nedorozumění.

Pokud připustíme integraci vlastní výpočetní techniky do školních sítí jako praxi, která je přínosná pro samotnou práci pedagogů i vzdělávací proces samotný, očekává se, že vytvoříme uživatelsky příjemné a bezproblémové prostředí sítě, ve které se buď uživatel cítit „jako doma“ a nebude mít problémy, které by jej odváděly od této praxe.

### **3.1. Přístup žáků k bezdrátovým technologiím**

Pokud je školské zařízení vybaveno bezdrátovou sítí, vzniká logický požadavek ze strany žáků na poskytnutí přístupu do sítě. Přístup k této problematice může být zdrojem rozsáhlých debat a diskuzí. Penetrace mobilních technologií mezi žáky jednoznačně stoupá, i když je závislá na konkrétní škole. Nejedná se pouze o notebooky, ale i mobilní telefony s funkcí připojení k bezdrátovým sítím, osobní digitální asistenty (PDA) a herní konzole. Zásadním aspektem pro povolení nebo zamítnutí přístupu k bezdrátové síti školy bude dopad na vzdělávací proces. V současné době v České republice probíhá hned několik výzkumných projektů, jejichž mise „je založena na zapojení žáků do procesu výuky interaktivní formou s využitím ICT prostředků“.<sup>1</sup> Jedním z nich je například „Vzdělání 21“, jehož odborným garantem je PF Univerzity Karlovy v Praze. Studie po dvou letech trvání projektu, kdy žáci mají prakticky neustálý přístup k informačním technologiím nejen ve výuce, ale i mimo ni, prokazuje, že stoupá aktivita žáků při vzdělávacím procesu,

---

<sup>1</sup> Cíle a vize >>Vzdělání 21<< [online]. 2010, 1, [cit. 2011-02-14]. Dostupný z WWW: <<http://www.vzdelani21.cz/cile-a-vize/>>.

jejich efektivnějším přístupem k informačním zdrojům, ale i odpovědnost při práci s počítačem a jeho využíváním. Vzhledem k relativně krátkému trvání projektu zatím neexistuje srovnávací studie výstupní úrovně znalostí a dovedností zapojených žáků a tříd s ostatními skupinami vzdělávanými tradičně.



*Mobilní počítačová učebna*

Přístup pedagogů, kteří se setkávají s negativními jevy, jako je zneužívání internetu, odvádění pozornosti od výuky chatováním pod lavicí a propadání závislosti na on-line připojení, bude zcela jistě odlišný a jejich nadšení pro zprostředkování přístupu k školní bezdrátové síti bude přinejmenším problematické.

Řešení není jednoduché a zcela jistě jej není možné postihnout černobílým soudem nebo konkrétním, vše postihujícím návrhem. Do značné míry bude opět záležet na každé škole, jejích dispozicích, celkovém klimatu a samozřejmě nastavených pravidlech. Je zřejmé, že na takových parametrech se bude diskuzí podílet celý sbor a přístup se bude vyvíjet v závislosti na získaných zkušenostech a poznacích. Pro potřeby projekce řešení bezdrátových sítí ve školském prostředí vyplývá fakt, že síť musí být připravena na rozmanitou škálu požadavků řízení přístupu, managementu a zabezpečení, které bude provozovatel (tedy škola) vznášet a od sítě očekávat.

### 3.2. Možnosti a rizika řízení bezdrátového přístupu k síti

Synonymem pro bezdrátové sítě se stalo tak zvané WiFi. WiFi (nebo také Wi-fi, WiFi, Wifi, wi-fi, wifi) je v informatice označení pro několik standardů IEEE 802.11 popisujících bezdrátovou komunikaci v počítačových sítích (též Wireless LAN, WAN). Název původně neměl znamenat nic, ale časem se z něj stal wireless free internet (bezdrátový volný internet), nebo též slovní hříčka wireless fidelity (bezdrátová věrnost) analogicky k Hi-Fi (high fidelity – vysoká věrnost). Původním cílem WiFi sítí bylo zajišťovat vzájemné bezdrátové propojení přenosných zařízení a dále jejich připojování na lokální (např. firemní) síť LAN. S postupem času začala být využívána i k bezdrátovému připojení do sítě Internet v rámci rozsáhlejších lokalit a tzv. HotSpotů.<sup>2</sup> WiFi zařízení jsou dnes prakticky ve všech přenosných počítačích a i v některých mobilních telefonech. WiFi zajišťuje komunikaci na linkové vrstvě, zbytek je záležitostí vyšších protokolů (na rozdíl například od Bluetooth, který sám o sobě zajišťuje nejrůznější služby). Jednoduše bychom mohli říci, že implementací WiFi vytvoříme neviditelný spoj mezi zařízením a aktivním síťovým prvkem, který je na úrovni tradičního strukturovaného metalického síťového rozvodu.

Zásadní těžiště problematiky přístupu uživatelů pomocí WiFi do lokální sítě je určení způsobu autentizace oprávněných uživatelů. Volba takového přístupu je záležitostí úzce spjatou s použitím takového připojení, prostředím, kde je technologie používána, připojovanými zařízeními a požadovanou mírou zabezpečení.

---

<sup>2</sup> Cisco Systems, Inc. Cisco BBSM Hotspot 1.0: User Guide. In: *Www.cisco.com* [online]. [cit. 2012-03-03]. Dostupné z: [http://www.cisco.com/en/US/docs/net\\_mgmt/cisco\\_building\\_broadband\\_service\\_manager/hotspot/1.0/user/guide/hs10\\_pf.html](http://www.cisco.com/en/US/docs/net_mgmt/cisco_building_broadband_service_manager/hotspot/1.0/user/guide/hs10_pf.html)



*Obecné schéma jednoduché sítě WLAN<sup>3</sup>*

### 3.2.1. Možnosti řízení přístupu k bezdrátové síti

Problém bezpečnosti bezdrátových sítí vyplývá zejména z toho, že jejich signál se šíří i mimo zabezpečený prostor bez ohledu na zdi budov, což si mnoho uživatelů neuvědomuje. Neoprávněný uživatel se může snadno připojit i do velmi vzdálené bezdrátové sítě jen s pomocí směrové antény, i když druhá strana výkonnou anténu nemá. Navíc většina nejčastěji používaných zabezpečení bezdrátových sítí má jen omezenou účinnost a dá se snadno obejít.

- **Zablokování vysílání SSID** (Service Set Identifier) sice porušuje standard, ale je nejjednodušším zabezpečením bezdrátové sítě pomocí jejího zdánlivého skrytí. Klienti síť nezobrazí v seznamu dostupných bezdrátových sítí, protože nepřijímají broadcasty se SSID. Bohužel při připojování klienta k přípojnému bodu je SSID přenášen v otevřené podobě a lze ho tak snadno zachytit.
- **Kontrola MAC adres** je metodou, kdy přípojný bod bezdrátové sítě má k dispozici seznam MAC adres (fyzických adres) klientů, kterým je dovoleno se připojit. Útočník se však může vydávat za stanicu, která je již do bezdrátové sítě připojena pomocí nastavení stejné MAC adresy (pokud je na AP tato funkce

---

<sup>3</sup> Obrázek: Malé domácí WiFi: Schéma WiFi sítě. In: PC Tuning [online]. [cit. 2012-03-28]. Dostupné z: [http://pctuning.tyden.cz/software/jak-zkrotit-internet/9381-rozvinte\\_svoj\\_internet\\_aneb\\_male\\_domaci\\_wifi](http://pctuning.tyden.cz/software/jak-zkrotit-internet/9381-rozvinte_svoj_internet_aneb_male_domaci_wifi)

aktivní). Navíc přístupový bod umožňuje většinou uložení pouze omezeného množství MAC adres.

- **802.1X** je protokol, pomocí nějž přístupový bod vyžaduje autentizaci. Pro ověření je používán na straně klienta program, který nazýváme suplikant, kterému přístupový bod zprostředkuje komunikaci s třetí stranou, která ověření provede (například tzv. RADIUS server).
- **WEP (Wired Equivalent Privacy)** je šifrování komunikace pomocí statických klíčů symetrické šifry, které jsou ručně nastaveny na obou stranách bezdrátového spojení. Díky nedostatkům v protokolu lze zachycením specifických rámců a jejich analýzou klíč relativně snadno získat. Pro získání klíčů existují specializované programy, které dnes již používají i malé děti.
- **WPA (WiFi Protected Access)** zabezpečení využívá kvůli zpětné kompatibilitě WEP klíče, které jsou ale dynamicky bezpečným způsobem měněny. K tomu slouží speciální doprovodný program, který nazýváme suplikant. Z tohoto důvodu je možné i starší zařízení WPA vybavit. Autentizace přístupu do WPA sítě je prováděno pomocí PSK (Pre-Shared Key – obě strany používají stejnou dostatečně dlouhou heslovou frázi) nebo RADIUS server (ověřování přihlašovacím jménem a heslem).
- **WPA2** je novější a přináší kvalitnější šifrování (šifra AES), která však vyžaduje větší výpočetní výkon, a proto nelze WPA2 používat na starších zařízeních.

### **3.2.2. Rizika přístupu k bezdrátové síti**

Bezdrátové sítě ve školském prostředí tvoří součást vnitřní infrastruktury školní sítě a jako takové by měly být zcela zabezpečeny proti přístupu neautentizovaných osob. Jedná se nejen o bezpečnost dat ve školní síti, ale i ochranu osobních dat a technologií tímto způsobem do sítě připojených. Z WiFi sítě se tak stává ve školském prostředí velmi specifický problém, ve kterém je třeba řešit individuální potřeby každé školy s ohledem na počet uživatelů, požadavky na jejich správu, ale i připojovaných zařízení a jejich možnostech a platformách. Při projekci konkrétního řešení je třeba zohlednit i stávající stav infrastruktury, zejména zabezpečení datových a aplikačních serverů, řízení přístupu k síťovým zařízením, jako jsou tiskárny a podobná zařízení, a před připojením bezdrátové části ověřit, zda neponecháváme náhodnému

návštěvníkovi otevřený přístup k těmto zdrojům. Zcela nezodpovědným přístupem je sdílení jednotných přístupových údajů větším počtem osob.

Každý uživatel takové sítě by měl být poučen o nebezpečích, která plynou z jejího používání, a o odpovědnosti za svěřené přístupové údaje, stejně tak jako odpovědnosti za data, která případně sdílí v rámci sítě. V sítích provozovaných na školách je zároveň velmi vysoké riziko pokusů žáků o získání práv a přístupů do oblastí s omezeným přístupem. Ve většině případů se jedná samozřejmě o čiročirou zvědavost a touhou zkusit, co dokážu, ale je třeba uvážit, že tyto pokusy mohou mít fatální následky pro provoz celé sítě, případně data na síti uložená. Z vlastní zkušenosti vím, že zvědavost žáků v oblasti informačních technologiích často přesahuje představivost správce školní sítě.

S touto problematikou úzce souvisí i bezpečnost instalované infrastruktury, zvláště v prostorách, kde k ní mají žáci volný přístup. Volba vhodných zařízení bude jistě nedílnou součástí projekční práce na projektu implementace WiFi sítě ve školním prostředí.

#### **4. Výzkum specifik školského prostředí**

V této části diplomové části se zkoumá současný stav informační infrastruktury na některých školách a požadavky ze strany učitelů, ICT koordinátorů, případně ředitelů škol. Analytická část rozebírá výsledky šetření, na nichž zakládá projekční část modelové realizace, rozboru vhodných technologií a požadavků, které by měly být splněny s ohledem na specifika, která se ve školách objevují a která se vymykají z běžně rozšířených řešení.

## 4.1. Šetření

Pro šetření současné vybavenosti a požadavků na další rozvoj informačních technologií byly vybrány školy různých typů s různou úrovní vybavenosti. Jednalo se o školy v Českých Budějovicích, tedy organizace zřizované magistrátem statutárního města České Budějovice nebo krajským úřadem Jihočeského kraje a jednu školu soukromou. Konkrétně

- Základní školu J. Š. Baara, pracoviště Jírovцова 9/a
- Základní školu J. Š. Baara, pracoviště Nová 5
- České reálné gymnázium s. r. o., Pražská 54a
- Gymnázium olympijských nadějí, Emy Destinové 46

Základní škola J. Š. Baara byla v roce 2005 sloučena se Základní školou Nová ulice pod jedno ředitelství. Provoz byl však zachován na obou pracovištích, která si zachovala odlišnou atmosféru i individuální přístup ke zkoumané problematice. Aby bylo prokázáno, že statistická data jsou relevantní i na takto malém vzorku, doplnil jsem je o informace dostupné ze strany České školní inspekce a Českého statistického úřadu. Tyto instituce oblast informačních technologií pravidelně zkoumají. Překvapivé je, že informace, které se týkají informačních technologií, se neobjevují na stránkách Ústavu pro informace ve vzdělávání, ačkoliv rovněž v rychlých šetřeních tyto oblasti sledují.

Česká školní inspekce prováděla celkem rozsáhlý výzkum v roce 2009. Tento monitoring probíhal téměř půl roku, a to od 1. února do 30. června 2009. Prozkoumáno bylo 463 základních škol. Cílem tohoto průzkumu bylo zjistit nejen vybavenost a využití ICT na základních školách, ale především i kvalitu tohoto materiálního vybavení. Základní jednotkou, díky níž se vůbec můžeme bavit o vybavenosti ICT na školách, je počet počítačů na 100 žáků. S tímto ukazatelem operuje právě Česká školní inspekce a pro srovnání jej budu používat i já.

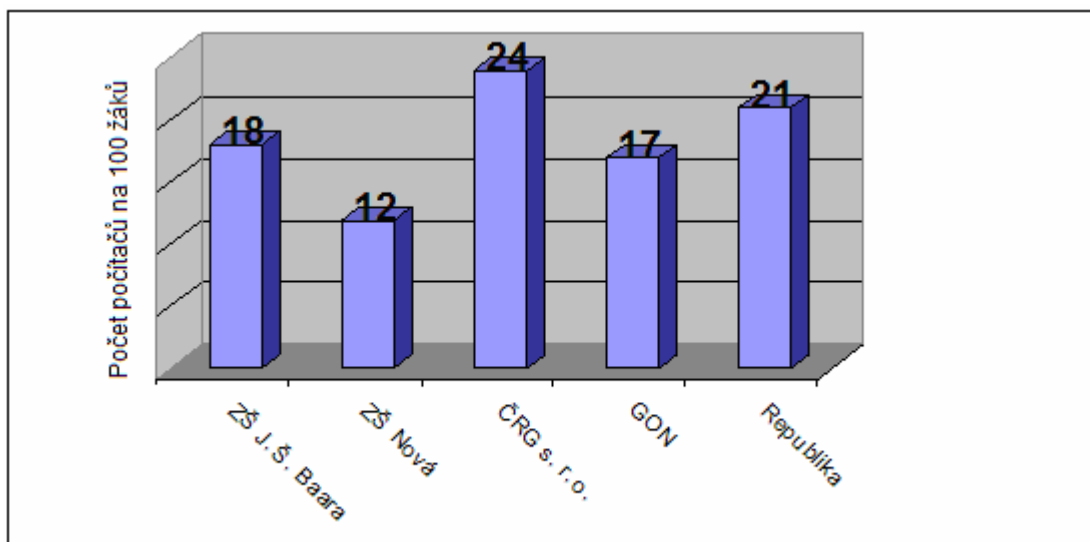
K výzkumu současného stavu informačních technologií na jednotlivých školách byl zvolen dotazníkový výzkum, který poskytl potřebná data a bylo možné jej jednoduše vyhodnotit a data zpracovat. Při zjišťování požadavků na rozšíření informačních technologií bylo zjištěno, že dotazník nepostihuje zcela požadavky, omezení a postřehy, které jsou pro práci podstatné. S ohledem na uvedené nedostatky

dotazníku byl zvolen osobní rozhovor vedený podle předem připraveného scénáře, který měl objasnit zjišťované skutečnosti. Těmito skutečnostmi bylo široké spektrum použitých technologií, které často dodávají formou outsourcingu externí firmy, a dále můj zájem o skutečnosti ovlivňující plánovaný rozvoj IT na školách. Jedná se o celou škálu faktorů, které by pouhým výčtem nepostihly celkovou situaci a záměry odpovědných pracovníků. Průvodní dopis k dotazníkovému šetření je uveden jako příloha diplomové práce.

## 4.2. Výsledky šetření

Data získaná z výzkumu bylo možné porovnat s výsledky, ke kterým dospěla Česká školní inspekce při svém šetření v roce 2009/10, které zveřejňuje na svých oficiálních stránkách a které používám jako referenční v dalším srovnání jako celorepublikový průměr.

Výsledky šetření, které proběhlo na již zmiňovaných školách, ukazují jen minimální rozdíly mezi celorepublikovým průměrem jak v oblasti vybavenosti, tak v oblasti připojení počítačů k lokální síti a potažmo k internetu.



*Počet PC na 100 žáků ve zkoumaných školách a celorepublikový průměr<sup>4</sup>*

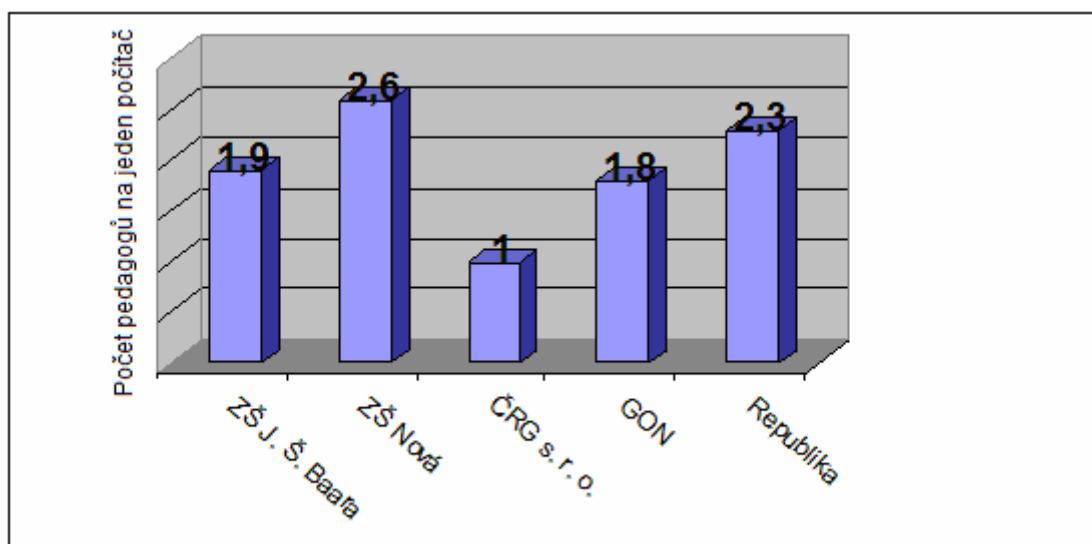
<sup>4</sup> Český statistický úřad, SRNSKÁ, Zuzana. Co říkají výzkumy a statistiky o vybavenosti ICT na základních školách. Online, 2010, s. 3.



Výsledky, které vzešly z porovnání údajů o počítačích připojených k LAN a internetu a počítačů bez připojení, jasně prokazují, že na školách jsou až na naprosté výjimky připojeny všechny počítače. Tyto výjimky jsou zpravidla počítače ponechané v provozu z historických důvodů a jsou tedy jakýmsi raritami.

Pro potřeby diplomové práce bylo dále zjišťováno, jakou část z celkového počtu žákovských počítačů tvoří notebooky. Výsledky ukazují, že na oslovených školách nemají žáci notebooky k dispozici. Výjimkou je České reálné gymnázium, kde 30% veškerých studentských počítačů tvoří tak zvaná mobilní učebna. Jedná se o sadu notebooků, které se používají disponibilně po celé budově napříč všemi vyučovacími předměty. Tímto se podle údajů České školní inspekce řadí České reálné gymnázium mezi 5 % škol v republice, které používají pro výuku studentské notebooky. Je třeba připomenout, že pro provoz takovéto mobilní učebny je třeba mimo jiné alespoň některé učebny vybavit příslušným rozvodem elektrické sítě pro napájení počítačů a to nemusí být místně proveditelné z hlediska stávajícího rozvodu.

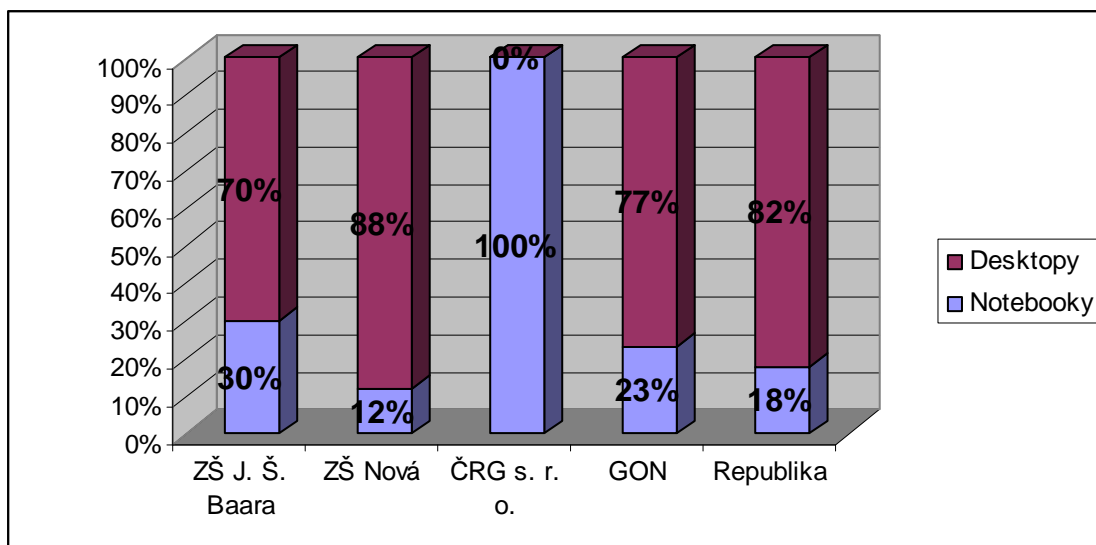
Zcela jinou kategorii tvoří informační technologie používané pedagogy. Zde je uveden přehled počtu pedagogů na jeden počítač:



*Počet pedagogů na 1 počítač ve zkoumaných školách a celorepublikový průměr<sup>5</sup>*

<sup>5</sup> Česká školní inspekce. *Úroveň ICT v základních školách v ČR* \*online. c2010, poslední revize 20. 11. Dostupné z: <<http://www.csicr.cz/cz/85156-uroven-ict-v-zakladnich-skolach-v-cr>>.

Dalším kritériem a předmětem výzkumu byl podíl notebooků a desktopů užívaných přímo pedagogy:



*Podíl notebooků a desktopů užívaných pedagogy*

Obecně lze hovořit o tom, že dostupnost informačních technologií pro pedagogy je celkem nízká, což potvrzuje i zpráva České školní inspekce: „Vzhledem k nezastupitelné roli ICT jakožto základního pracovního prostředku (obzvláště ve vzdělávání) lze díky výše uvedenému zjištění tvrdit, že naprostá většina učitelů nemá dostatečné podmínky pro výkon své profese.“<sup>6</sup>

Výjimkou je České reálné gymnázium, které již několik let zpracovává veškerou školní agendu elektronicky. V praxi to představuje fakt, že každý pedagog má přidělen notebook, který nahrazuje třídní knihu, každý pracovník školy je dále povinen bez prodlení zaznamenávat elektronicky veškerou klasifikaci. Pomocí rozšířeného systému pro školskou agendu Bakaláři umožňuje žákům i jejich rodičům sledovat výsledky vzdělávání, absenci, rozvrh a jeho změny a slouží víceméně i jako komunikační prostředek.

Již zmíněný systém Bakaláři je instalován na všech zkoumaných školách. Vzhledem k množství modulů, kterými systém disponuje, je však používán různým způsobem, většinou jako evidenční systém a také pro tisk vysvědčení. Hlavním

<sup>6</sup> Česká školní inspekce. *Úroveň ICT v základních školách v ČR \*online+.* c2010, poslední revize 20. 11. 2010  
Dostupné z: <<http://www.csicr.cz/cz/85156-uroven-ict-v-zakladnich-skolach-v-cr>>.

markantem systému Bakaláři je fakt, že v současné době podporuje výhradně platformy firmy Microsoft. Vývoj univerzálního rozhraní na bázi PHP byl zastaven, což osobně považuji za nešťastné.

### **4.3. Požadavky na řešení**

Výsledky šetření, které proběhlo na již zmiňovaných školách, potvrzují fakt, že odpovědní pracovníci vnímají nárůst požadavků na bezdrátová připojení používaných počítačů. Jedná se v první řadě o počítače pedagogů, od kterých se čeká v brzké době zpracovávání povinné školské dokumentace elektronicky. Z přímých rozhovorů se správci i řídicími pracovníky zaznívá prakticky jednomyslný názor vyjadřující přesvědčení, že při dalším realizovaném obnovování výpočetní techniky, kterou mají k dispozici pedagogové, budou preferovat notebooky připojené ke školní síti bezdrátově.

Školská zařízení vyšších stupňů, tedy střední školy, by uvítala možnost zpřístupnění internetu studentům za předpokladu, že by tento přístup byl jmenovitě řízený a monitorovaný na úrovni objemové statistiky množství přenesených dat. Takový přístup by musel být logicky oddělen od provozní sítě tak, aby ji nenarušil z hlediska množství připojených počítačů a omezení přenosové kapacity.

Dalším aspektem, na kterém se shodli všichni dotázaní, jsou nepochybně finance. Systémy financování školského resortu se neustále mění, stejně jako množství přidělovaných prostředků, což do značné míry komplikuje možnost dlouhodobého (ale v podstatě i střednědobého) plánování v kapitole tak finančně výrazné, jako jsou informační technologie. Finanční náročnost projektů spojených s rozšiřováním infrastruktury o bezdrátové prvky je tedy determinována možnostmi konkrétního školského zařízení. Výsledkem je tedy několik bodů, které musí řešení splňovat, aby bylo použitelné ve školách:

- Modularita
- Možnost oddělení sítí podle použití (provozní a žákovská)
- Jmenovité řízení přístupu uživatelů
- Nezávislost na platformě technologií stávající sítě
- Finanční (ne)náročnost

## 5. Dostupné technologie

Šíře trhu v oblasti technologií poskytujících řízení přístupu k síti, potažmo bezdrátové síti, je poměrně vleká. Prakticky každým dnem se objevují další zařízení a rovněž pořizovací cena se neustále mění v závislosti na jejich rozšíření a běžné užitnosti. S ohledem na tato fakta je tato kapitola pouze orientačním návodem, jakousi poznámkou, které parametry byly při realizaci zohledňovány a které mohou mít vliv na celkový systém a jeho užitnou hodnotu. Je pravděpodobné, že tato informace bude časem znehodnocována spolu s nástupem nových trendů a přístupů k řešení zadaného problému.

### 5.1. Rozbor dostupných technologií

Tato část je pojata názorně. Na základě zjištěných požadavků v rámci teoretické části práce byly vybrány technologie, které jsou podrobeny rozboru z hlediska použitelnosti pro modelovou aplikaci. Jsou hodnoceny z pohledu modularity, umožnění řízení sítí v rovině oddělených provozních a žákovských sítí, nezávislosti na platformě již realizovaných částí sítě a v neposlední řadě ceny.

#### 5.1.1. 2.4GHz 54 Mbps Wireless SMC EliteConnect Hotspot Gateway

Toto zařízení je podle dostupných statistik nejprodávanějším zařízením představujícím tak zvané all-in-one řešení. Podle technické specifikace výrobce poskytuje:

- Zabezpečený přístupový bod do internetu
- Vysokorychlostní bezdrátový přístup do LAN
- Autentifikační a účtovací služby pro připojené klienty
- Přímý tisk distribučních lístků s přihlašovacími údaji



*2.4GHz 54 Mbps Wireless SMC EliteConnect Hotspot Gateway*

Výrobce sám uvádí, že se jedná o technologii doporučenou pro distribuci bezdrátových sítí v provozech, jako jsou kavárny, restaurace, hotelové recepce a podobně. Správa účtů v takových zařízeních je realizována většinou tak, že klient dostane vytištěný lístek s přístupovými údaji, který je časově omezen na dobu nastavenou správcem. Po této době platnost účtu vyprší a tento se zamkne a následně vymaže z databáze účtů. Nutno zmínit, že obsluhu zvládne i osoba, která nemá o práci s technikou sebemenší ponětí, protože se tato činnost omezuje na stisknutí tlačítka a odebrání lístku.

SMC EliteConnect je vybaven bezdrátovým rozhraním v pásmu 2,4GHz, včetně antén o zisku 2dB, dále čtyřmi porty 10/100Mbps použitelnými jako switch a WAN portem (10/100Mbps). Přes rozhraní HotSpotu je možný i management klientů připojených přes čtyři zmíněné drátové porty. Tady by byl prostor pro připojení dalších bezdrátových přístupových bodů, které by zcela bez zabezpečení přenechaly řízení přístupu SMC EliteConnectu. Není tedy pravda, že pro pokrytí většího prostoru by bylo třeba několik takových zařízení, právě naopak, tento HotSpot lze doplnit a infrastrukturu rozšířit o další přístupové body. Značnou nevýhodou je, že zařízení neumožňuje propojit připojované zařízení přes WAN port do sítě přes Bridge. Tím znemožňuje vytvoření dvou kolizních domén a následně není možné využívat služby běžící například na stávajícím serveru jako jsou doména, ActiveDirectory (u MS serverů), nebo přímý přístup k databázovým serverům.

Takový požadavek se ve školském prostředí ale často objevuje právě z důvodu práce s programy a systémy běžícími na stávajících serverech a služeb dostupných v stávajících školních sítích. Zdánlivě jednoduchý by byl management účtů a správa

uživatelů. Vydávané lístky by byly zcela anonymní a monitoring sítě by byl prakticky nemožný. Cílené zamezení přístupu konkrétního uživatele nebo skupiny uživatelů by bylo prakticky nemožné.

Ve prospěch aplikace tohoto zařízení jednoznačně hovoří nenáročnost na obsluhu, robustní řešení a renomovaný výrobce. Technologie by obstála ve školském prostředí v případě, že by se jednalo o aplikaci polokomerční (ve školním bufetu by si žák zakoupil například jednodenní přístup za pět korun), jejíž provoz není monitorován a žáci mají přístup řízen pouze souhrnem obecných pravidel pro použití sítě. Výstavba by v tomto případě byla banálně jednoduchá, možnosti rozšíření a zvyšování pokrytí prakticky neomezené.

Proti nasazení hovoří zejména fakt, že se jedná o proprietární zařízení bez nejmenší možnosti vyššího zásahu do organizace a řízení sítě. Zmíněná nemožnost připojení tzv. Bridgem ke stávající síti prakticky vylučuje aplikace závislé na doméně a jiných službách běžících na serveru. Zjednodušený přístup a předem vymezený model použití je v tomto případě jednoznačně na škodu. Dalším kritériem je cena zařízení, která v době zpracování projektu činila cca 16 000,- Kč. Vzhledem k výše popsaným negativům je zřejmé, že pro školský sektor, kde se nedá předpokládat návratnost investice, je poměr cena/přidaná hodnota nevhodně vysoký.

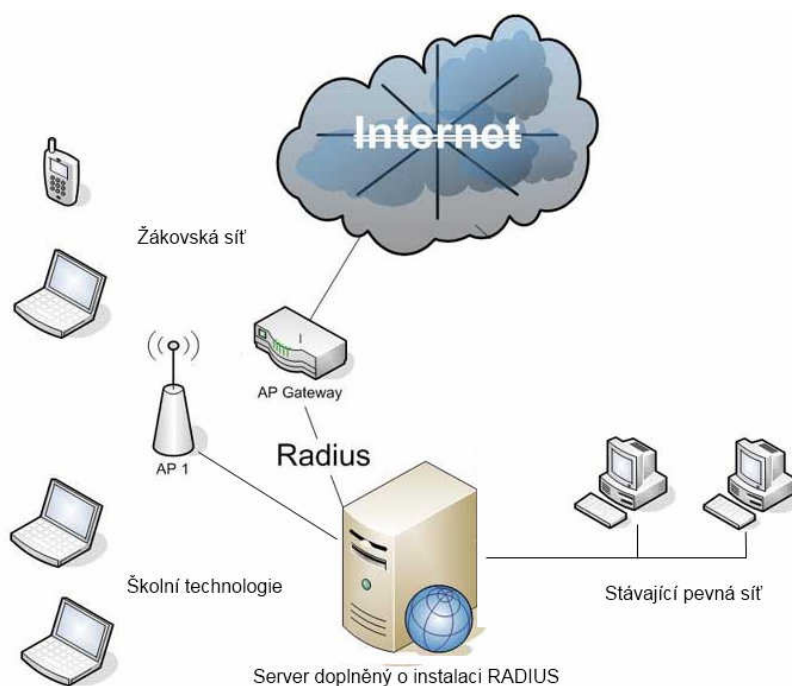
Technologie Wireless SMC EliteConnect Hotspot Gateway je typickým představitelem rodiny all-in-one řešení, kterých na trhu najdeme celou řádku. Bohužel jsou předem připravené (většinou velmi sofistikovaně) pro komerční aplikace a ve většině případů je nelze aplikovat na zadání vzešlé ze školského prostředí.

### **5.1.2. TekRADIUS server pro Windows**

V tomto případě se jedná o software aplikovaný na stávajícím serveru provozovatele. Samotný RADIUS server je jako funkce obsažen i v distribuci Windows Server 2003, která pracuje i v modelové síti. Vzhledem ke snaze o modulární a zejména univerzální pojetí projektu, byl pro posouzení zvolen samostatný software nezávislý na verzi operačního systému na serveru. Nejprve krátce o problematice RADIUSu.

**RADIUS** (Remote Authentication Dial In User Service, česky Uživatelská vytáčená služba pro vzdálenou autentizaci) je protokol používaný pro přístup k síti nebo pro IP mobilitu. Mezi nejdůležitější vlastnosti patří jeho vysoká síťová bezpečnost, neboť transakce mezi klientem a RADIUS serverem je autentizována pomocí sdíleného tajemství, které není nikdy posíláno přes síť. Všechny uživatelská jména jsou přes síť zasílána šifrovaně.

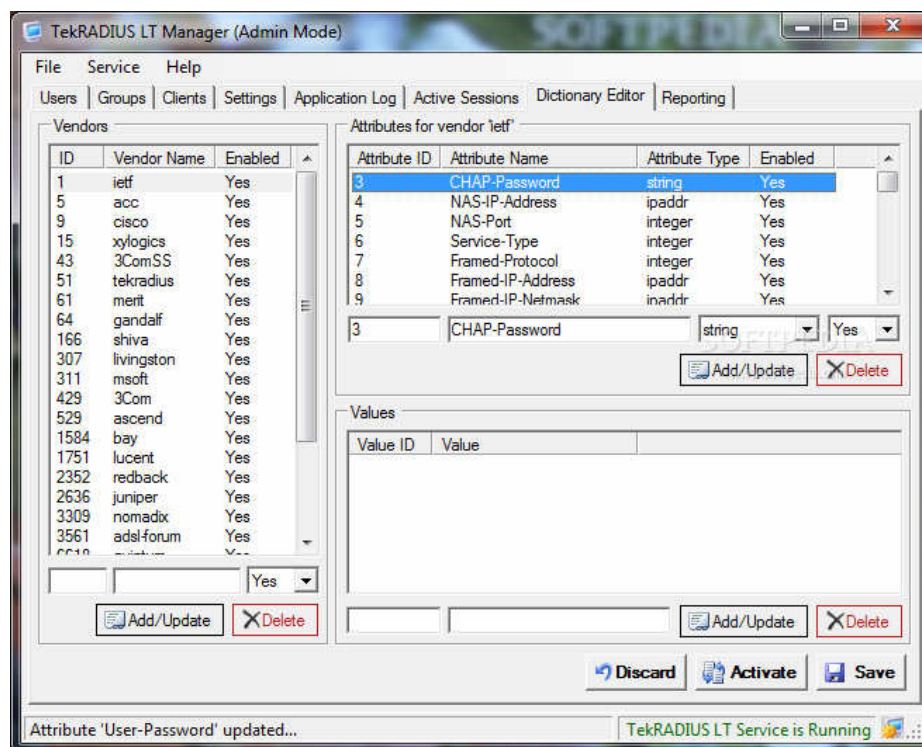
Postup autentizace je následující: uživatel vydá klientovi *Požadavek na autentizaci*, klient vytvoří *Požadavek na přístup* (Access Request) obsahující uživatelské jméno, heslo a ID portu, přes který je uživatel připojen. Požadavek na přístup je odeslán RADIUS serveru a čeká se na odpověď. Pokud nepříjde do určeného času (timeoutu) žádná odezva, Požadavek na přístup se opakuje, zpravidla 3 až 5 krát. Pokud není splněna některá z podmínek, RADIUS server odešle *Zamítnutí přístupu* (Access Reject). Jestliže jsou všechny podmínky splněny, RADIUS server odešle *Povolení přístupu* (Access Accept), kde v datové oblasti paketu jsou uloženy všechny potřebné konfigurační informace (IP adresa, maska sítě, login uživatele a vše, co je potřeba předat požadované službě).



### *Aplikace RADIUS do prostředí školy s realizovaným zadáním<sup>7</sup>*

<sup>7</sup> Ilustrace - hotspot.jpg. In: *Aradial Wi-fi Technologies Ltd.* [online]. [cit. 2012-03-24]. Dostupné z: <http://www.wifi-radius.com/images/hotspots.jpg>

V praxi je nejčastěji používán u menších lokálních poskytovatelů. Při připojení k poskytovateli internetu pomocí WiFi je u některých poskytovatelů vyžadováno přihlašovací uživatelské jméno a heslo. Tato informace je poslána do takzvaného Network Access Server (NAS) zařízení přes Point-to-Point Protocol (PPP). Poté je předána RADIUS serveru přes RADIUS protokol. Pokud je uživatelské jméno a heslo přijato, server autorizuje přístup k poskytovateli internetu a vybere IP adresu (popřípadě rozsah adres) a další parametry spojení, což mohou být např. přihlašovací údaje, doba, po kterou může být uživatel připojen, rychlost připojení, kterou může uživatel používat, nebo jiná omezení. RADIUS server bude také upozorněn na spuštění nebo ukončení sezení, takže informace mohou být použity pro statistické účely.<sup>8</sup>



*Aplikace TekRADIUS v provozu na Windows Server 2003*

Výhodou tohoto řešení je jednoznačně zachování investic, obrovská modularita a šířka nabízených služeb. Konkrétně při aplikaci na modelové škole se mi podařilo provázat operační systém serveru (Windows Server 2003) a jeho službu

<sup>8</sup> GNU's Not Unix!: Radius. *GNU's Not Unix!* [online]. [cit. 2012-03-17]. Dostupné z: <http://www.gnu.org/software/radius/>



ActiveDirectory pro správu uživatelů, takže při editaci práv uživatelů bylo možné řešit i možnosti jejich přístupu ke školní síti a potažmo k internetu. Zmíněný software TekRADIUS umožňuje tato práva doplnit. Pro školní počítače a počítače pedagogů se mi podařilo vygenerovat certifikáty, které po instalaci umožnily z takto ošetřených počítačů přístup přes WiFi bez nutnosti neustálého zadávání identifikačních údajů. Cena takového software se pohybuje v řádech 500 - 3000,- Kč, což není částka pro školské zařízení nereálná. Ve zkratce ideální stav umožňující vše, co by mohl zadavatel vymyslet.

Nevýhoda se však objevila při pokusu sestavený model distribuovat a nabídnout k realizaci na jiném školském zařízení. Jistě by bylo možné vyřešit problémy s obrovskou škálou operačních systémů, které jsou na školách instalovány (od MS Windows nejrůznějších verzí a tedy i možností po obrovskou škálu Unixových systémů a Linuxových distribucí). Jistě by bylo možné v obrovské nabídce programů, jako je TekRADIUS, nalézt vhodné řešení podle konfigurace, požadavků a možností každé školy. Jistě by se našlo i řešení pro malé školy, které třeba ani nemají server.

Zde je ale na místě zdůraznit, že cílem této diplomové práce je návrh zcela modulárního (co do požadavků zadavatele) a univerzálního (bez ohledu na platformu a stávající infrastrukturu) řešení, které by bylo možné jednoduše použít prakticky všude. Takové řešení tedy popsáním jednoho programu nevyřešíme. Zároveň nejsou výjimkou případy, kdy škola má síťové služby dodávané externí firmou (tzv. Outsourcing) a zaměstnanci školy k serveru a jeho managementu nemají přístup, nebo správu realizují pomocí aplikace pro správu domény.

### **5.1.3. OS MikroTik a MikroTik Router Board**

O komplexním řešení na bázi MikroTik jsem se dozvěděl v roce 2007 z nadšených debat zaměstnanců a majitelů lokálních ISP (Internet Service Provider). Modularita, šířka použití a dostupnost všem velice imponovala. V pravém slova smyslu se jedná o operační systém na bázi Linuxu kompilovaný s ohledem na provoz síťových služeb. Výrobce zároveň dodává celou širokou škálu tak zvaných Router Boardů s před instalovaným operačním systémem, které přímo vybízí k aplikaci. Operační systém je však dostupný i pro x86 architekturu a díky tomu ho můžeme

nainstalovat na prakticky jakýkoli počítač. Router Boardy vynikají především svou kompaktností, robustním řešením (odolnost proti přepětí, široké pásmo provozních teplot), nízkou spotřebou a cenou. Ta se pohybuje u použitelných Router Boardů do 1000,- Kč a to včetně předinstalovaného operačního systému umožňujícího předpokládané aplikace ve školském prostředí.

A právě z těchto poznání se začala rodit myšlenka sestavit několik modulů, ze kterých by si škola dokázala vybrat právě ty, které jsou podle specifických požadavků vhodné a nezávisle na použitých technologiích či formě původní infrastruktury aplikovatelné.



*Ilustrační foto RouterBoardu RB532*

Pro toto řešení hovoří naprosto jednoznačně obrovská modularita, šíře a otevřenost všech dostupných nastavení, která si jen můžeme v malé síti přát, a cenová dostupnost, která bude při realizaci také určující. Jednoduchou zálohou konečné konfigurace je možné distribučně poskytnout všem zájemcům již nastavené zařízení, které si uživatel přizpůsobí už jen kosmeticky místním potřebám (IP rozsah a podobně).

Nevýhody pro uživatele prakticky neexistují. Pro programátora, který konkrétní řešení sestavuje, je nezbytností zorientovat se v dostupných funkcích, kde může být paradoxně jejich obrovské množství ze začátku překážkou. Dostupné materiály jsou převážně anglicky. Tato fakta však neuvádím jako zásadní argumenty proti aplikaci, protože jsou u podobných technologií běžná.

## 5.2. Výběr technologie

Výběr byl tedy na základě výše uvedených faktů nakonec víceméně jednoznačný. Na platformě MikroTik bude realizována funkční základna pro připojování jednotlivých zařízení do sítě tak, aby bylo každé zařízení zvlášť identifikováno a připojeno buď do žákovské virtuální sítě, nebo školní provozní sítě s přímým přístupem na školní aplikační a SQL server. Žákovská síť bude navíc opatřena přístupovou HotSpot stránkou, která bude vyžadovat autentifikaci každého uživatele pomocí personálně vytvořeného uživatelského účtu. Takto bude možné pomocí softwarových záloh vytvořit zvláštní modul pro žákovskou infrastrukturu s přístupovým HotSpotem, modul pro vytvoření provozní infrastruktury pro připojení školní techniky a počítačů pedagogů, nebo oba uvedené moduly kombinovat. To umožní správcům sítě určit rozsah použití a zpřístupnění bezdrátové sítě jimi požadovanému okruhu osob správcem uvedeným způsobem.

## 5.3. Platforma MikroTik

Tato kapitola přibližuje platformu pro realizaci projektu. Je určena zejména správcům, kteří by chtěli dále specificky upravovat dále popsané nastavení, nebo by chtěli platformu využít pro jiné síťové aplikace.

O výrobci se můžeme dozvědět: MikroTiks (tikls = síť; ve světě známá zejména jako MikroTik) byla založena v roce 1995 k vývoji a prodeji bezdrátových systémů zejména pro ISP. Nyní poskytuje bezdrátové systémy pro internetovou konektivitu v mnoha zemích po celém světě. Společnost se nachází v Lotyšsku.<sup>9</sup>

Jak už bylo popsáno výše, často se nesprávně za MikroTik považuje zejména řada tak zvaných RouterBoardů, které společnost dodává. Jedná se však primárně o distribuci síťového operačního systému na bázi Linuxu. Často kritizovaným faktem je, že ačkoliv zde naleznete veškeré myslitelné programy, které z linuxových distribucí znáte, neumožňuje MikroTik OS přidání vlastních aplikací. Operační systém je distribuován v několika třídách (Levelch) podle použití a rozsahu požadovaných funkcí. Podle obecných zkušeností je pro všechny potřeby malých sítí adekvátní Level 4, který je také nejčastěji součástí dodávaných RouterBoardů a jehož licence je již v ceně hardwaru. Při nákupu nového RouterBoardu se doporučuje aktualizace na

---

<sup>9</sup> MikroTik: MikroTik. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2010, 29.4.2011 [cit. 2012-02-18]. Dostupné z: <http://cs.wikipedia.org/wiki/Mikrotik>

nejnovější verzi příslušného operačního systému z důvodu až překotného vývoje. Jen zřídka se stává, že při aplikaci zálohy nastavení dojde ke špatné interpretaci skriptu z důvodu přechodu na novou verzi, ale tuto eventualitu nelze zcela vyloučit. V následující tabulce je stručný přehled verzí operačního systému MikroTik.<sup>10</sup>

Level number	0 (FREE)	1 (DEMO)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Upgradable To	-	no upgrades	ROS v4.x	ROS v4.x	ROS v5.x	ROS v5.x
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h limit	-	-	yes	yes	yes
Wireless Client, Bridge	24h limit	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h limit	-	yes	yes	yes	yes
EoIP tunnels	24h limit	1	1	unlimited	unlimited	unlimited
PPPoE tunnels	24h limit	1	1	200	500	unlimited
PPTP tunnels	24h limit	1	1	200	unlimited	unlimited
L2TP tunnels	24h limit	1	1	200	unlimited	unlimited
OVPN tunnels	24h limit	1	1	200	unlimited	unlimited
VLAN interfaces	24h limit	1	1	unlimited	unlimited	unlimited
P2P firewall rules	24h limit	1	1	unlimited	unlimited	unlimited
NAT rules	24h limit	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h limit	1	1	200	500	unlimited
RADIUS client	24h limit	-	yes	yes	yes	yes
Queues	24h limit	1	unlimited	unlimited	unlimited	unlimited
Web proxy	24h limit	-	yes	yes	yes	yes
User manager active sessions	24h limit	1	10	20	50	Unlimited

*Přehled verzí OS MikroTik*

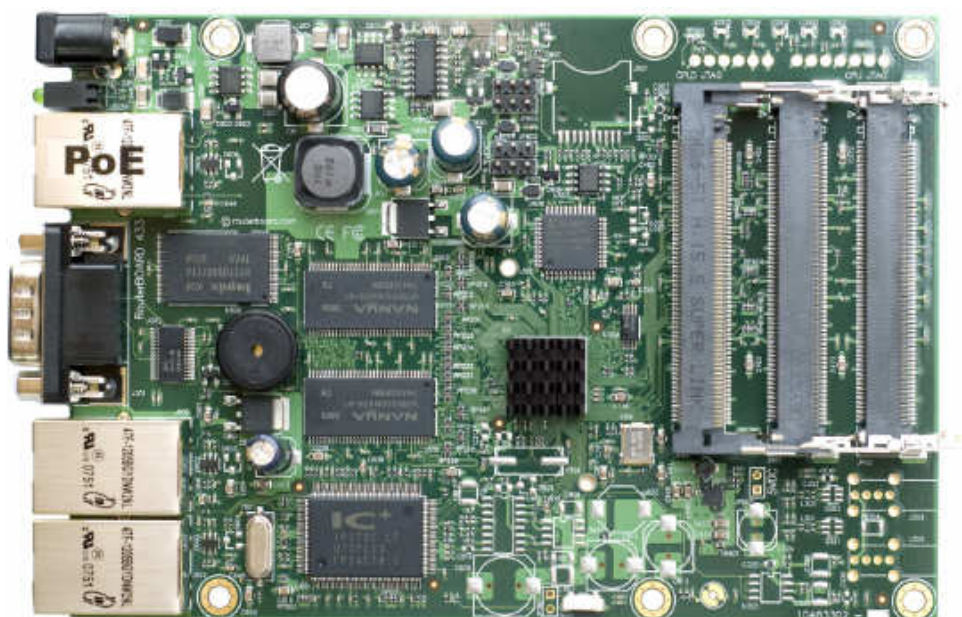
Modely RouterBoardů se liší především výkonem, licencí ROS a možnostmi rozšíření. V neposlední řadě to je také spotřeba a velikost celého zařízení. Některé modely se dají dále rozšiřovat o další miniPCI sloty a ethernetové porty. Největším rozdílem je ale rychlost CPU, která je největším limitem pro připojení klientů na RouterBoard.

RouterBoard se určením dělí do několika řad, které se liší právě rychlostí procesoru a velikostí paměti. Každá řada je tak určena k něčemu jinému.

<sup>10</sup> What is router OS: OS MikroTik. In: [Http://www.mikrotik.com/pdf/what\\_is\\_routeros.pdf](http://www.mikrotik.com/pdf/what_is_routeros.pdf) [online]. [cit. 2012-02-18]. Dostupné z: [http://www.mikrotik.com/pdf/what\\_is\\_routeros.pdf](http://www.mikrotik.com/pdf/what_is_routeros.pdf)

<b>RB 1xx</b>	Dnes je již nevyrobí a maximálně se dají nakoupit skladové zásoby. Jedná se o nejslabší řadu RB od Mikrotiku určenou převážně ke klientům. Modely se dají osadit až třemi WiFi kartami a obsahují až tři ethernet porty (model 150 jich měl 5). Tato řada byla nahrazena modely 411, případně 433.
<b>RB 3xx</b>	Dnes se již také nedá sehnat, ale je stále součástí mnoha páteřních spojů a najdeme ho také u množství klientů, kteří potřebovali připojit více než jen pár počítačů.
<b>RB 4xx</b>	Nová řada nahrazující modely z řad 1xx a 3xx. Přináší především rychlejší procesor a více paměti. V této řadě můžeme najít jak modely určené pro domácí použití, tak pro nasazení na středně zatížené spoje.
<b>RB 6xx</b>	Pro páteřní spoje o několika desítkách uživatelů je řada 6xx jako stvořená a s možností rozšíření je možné tyto karty osadit až osmi WiFi kartami.
<b>RB 10xx</b>	Nejvýkonnější řada a také s patřičnou cenou. Hodí se především v kombinaci s 1 Gbit/s ethernetem. RB této řady můžeme umístit do racků.

Tabulka neobsahuje všechny řady, které Mikrotik měl či má, ale pouze ty, se kterými se dá při běžném používání setkat.<sup>11</sup>



*Mikrotik RouterBoard RB433AH*

Rychlost procesoru je pro RouterBoardy nesmírně důležitá, pokud si uvědomíme, že veškeré procesy probíhají softwarově. Veškerá řízení přístupů, filtry a skripty budou zatěžovat procesor a zátěž bude stoupat s každým připojeným

<sup>11</sup> ŠTRAUCH, Adam. Mikrotik: Seznámení s Wi-Fi krabičkou. In: *Www.root.cz* [online]. 7. 11. 2008 [cit. 2012-02-18]. Dostupné z: <http://www.root.cz/clanky/mikrotik-seznameni-s-wi-fi-krabickou/>

uživatelé. I v menší škole (cca 300 žáků) se může běžně stát, že v témže okamžiku bude připojeno 70 uživatelů.

Pro realizaci modelového řešení však nabízí trh variantu sice ořezanou o možnosti modulárního rozšiřování, které nabízí výše popsané řady, ale zato bez nutnosti pořizování zdroje, racku a dalších nákladových položek. S přihlédnutím k tomu, že pro projektový záměr nám bude stačit RouterBoard s několika konfigurovatelnými síťovými porty, dostatečně výkonným procesorem a pamětí 64MB, bude řada těchto RouterBoardů v kompaktním zapouzdřeném provedení bohatě postačovat. Aplikace bude tedy přizpůsobena možnostem MikroTik RouterBoard RB750. RouterBoard MikroTik RB750 je boxový router s 5 Ethernet porty založený na MikroTik RouterOS Level4. Router v plastovém case disponuje 5 LAN porty 10/100 Mbps, z nichž jeden umožňuje proprietární napájení po Ethernetu PoE. Router není vybaven sériovým portem, dodáván je s externím napájecím zdrojem.

Technická specifikace:

DHCP: ano

LAN port: 5 x RJ45 10/100 Mbps MDI/MDI-X

NAND: 64MB

Napájení: JACK + POE (10-28 V)

Procesor: Atheros AR7240 400MHz

Provozní teplota: -20 až 60 °C

RAM: 32 MB SDRAM

Rozhraní: LAN

Rozměry: 113 x 89 x 28 mm

Hmotnost: 0.25 Kg

LED indikace: ano

OS: MikroTik - RouterOS v3 Level 4

## **6. Realizace**

Tato část diplomové práce má za cíl popsat kroky, které vedly k realizaci projektu školní bezdrátové sítě na základě analýzy požadavků konkrétního školského zařízení. Požadavky byly stanoveny na základě seznámení zadavatele s problematikou, možnostmi a průzkumu stávající infrastruktury a dostupnými technologiemi. Součástí zadání je v neposlední řadě rozpočet, který pochopitelně zajímá každého zřizovatele v oblasti školství a který je rovněž závazný.

### **6.1. Projekční zadání**

Modelovou školou se stalo České reálné gymnázium s. r. o. v Českých Budějovicích, a to zejména ze tří důvodů. Jednak tato škola dlouhodobě usilovala o zprovoznění povinné školské agendy elektronickou formou, což předpokládá přístup vyučujících ke školní síti prakticky v každé učebně školy. Dále zde s nástupem mobilních technologií začal sílit tlak na zpřístupnění internetu pro žáky školy a samozřejmě individuálního řízení přístupu jednotlivých studentů, jak je popsáno již v teoretické části diplomové práce. Posledním důvodem je fakt, že jsem zaměstnancem této školy, takže výsledek projektu mohu dlouhodobě testovat a vznikne tak silná a relevantní zpětná vazba z provozu.

#### **3.1.1. Stávající infrastruktura - výchozí podmínky**

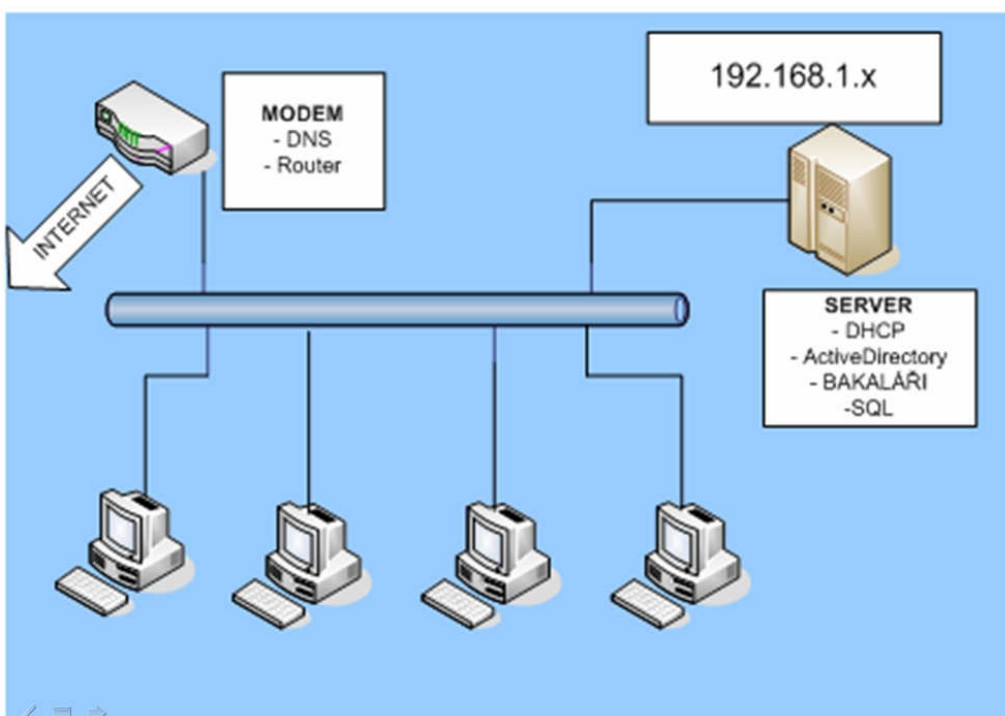
České reálné gymnázium má pevnou lokální síť s částečným rozvodem po budově, server s operačním systémem Windows 2003 Server s aplikovanou doménou a ActiveDirectory serverem pro správu uživatelských účtů. Nosnou aplikací instalovanou na serveru je software pro školskou agendu Bakaláři a jí využívaný MSSQL databázový server. Škola je připojena k internetu širokopásmovým připojením ADSL 25 Mbps. V budově jsou rovněž dvě učebny s pevnými počítači. Pro potřeby výuky je k dispozici 15 notebooků. Ve všech učebnách je po obvodové zdi elektroinstalace umožňující připojení notebooků do elektrické sítě. Na třech místech budovy jsou umístěny WiFi přístupové body (dále AP) připojené tak zvaným bridgem do školní sítě. Přístup je omezen filtrem MAC adres. Toto zabezpečení se jeví jako

nedostatečné, protože bylo prokázáno, že někteří zvědaví studenti si opsali MAC adresy z žákovských notebooků, simulují je na své technice a získávají tak přístup k internetu bez povolení provozovatele sítě.

### **6.1.1. Požadavky na projektové řešení**

Zadáním projektu je stávající stav doplnit o bezdrátové připojení dostupné po celé budově. Vzniknout by měly dvě bezdrátové virtuální sítě. První z nich by byla přímo přemostěná (Bridge) do školní sítě v jejím adresním rozsahu, poskytovala by přístup do domény serveru, databázového serveru a bezchybný chod systému Bakaláři. Přístupná by byla pouze zařízením pedagogů a byla by rovněž využita pro připojení mobilních učeben realizovaných notebooky. Druhá by byla virtuální síť s vlastním adresním rozsahem a individuálním řízením přístupu uživatelů, která by byla k dispozici registrovaným studentům pro přístup k internetu. Registrovanému studentovi by přístup do sítě umožnilo zadání unikátního přístupového jména a hesla. Přístup ke správě takto zřízených kont by měl mít pověřený pracovník. Rozhraní pro správu by mělo být přehledné a srozumitelné i pracovníkovi s běžnou informační gramotností. Předpokládá se maximální využití stávající infrastruktury, dodržení všech bezpečnostních norem a samozřejmě dodržení finančního limitu stanoveného pro kompletní realizaci na 35 000,- Kč.





Obr. 4. Stávající stav na ČRG s.r.o.

## 6.2. Projekce

V celkovém souhrnu požadavků zadavatele je technicky význačná realizace dvou nezávislých bezdrátových sítí. Jedna provozní, sloužící pro připojení školních počítačů a technologií používaných pedagogy, a druhá zabezpečená HotSpotem pro připojení zařízení studentů.

V případě provozní sítě se předpokládá plná spolupráce s doménou na stávajícím serveru (platforma Microsoft viz stávající infrastruktura) a tamtéž nainstalovaném systému pro školskou agendu Bakaláři, která využívá dat uložených na MS SQL serveru. Je tedy žádoucí, aby se počítač připojený do této sítě adresoval DHCP serverem ve stejném rozsahu adres, jako ostatní počítače ve stávající síti. Bude se tedy jednat o případ, kdy jednotlivé přístupové body přenáší konkrétní připojení tak zvaným Bridgem. Bridže, někdy zvaný brouter, rozděluje síť na dvě kolizní domény. Umožňuje stanicím v kterékoliv síti přistupovat na zdroje v druhé síti. Pomocí mostů je možné prodlužovat délku, počet uzlů v síti a redukovat úzké profily vzniklé z přílišného počtu připojených počítačů.<sup>12</sup> Zabezpečení dat je možné realizovat na

<sup>12</sup> Počítačové sítě: Bridge. In: *Počítačové sítě: site.the.cz* [online]. 1.1. [cit. 2011-10-25]. Dostupné z: <http://site.the.cz/index.php?id=9>

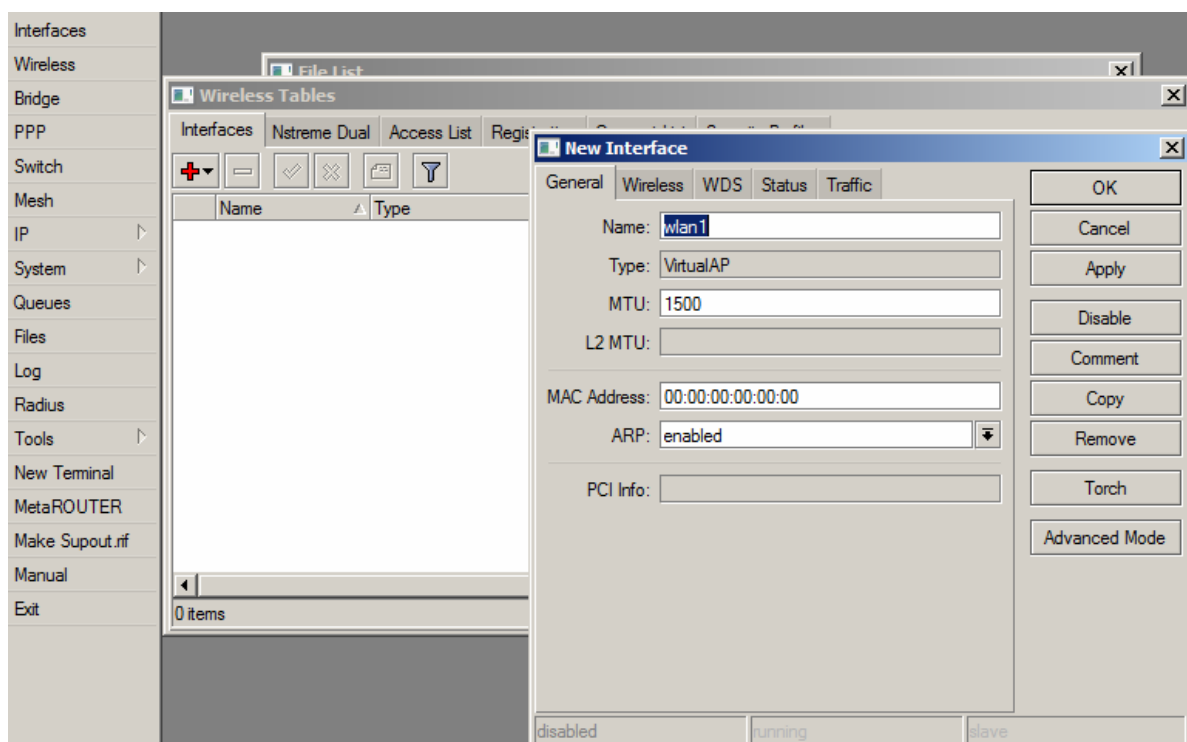
straně serveru, případně i na straně přístupového bodu. Samotné bezdrátové spojení je zde pouze linkovým řešením.

Žákovská síť pak řeší pouze řízení přístupu k Routeru připojujícího školu k vnější síti, tedy internetu. Tato bezdrátová síť může mít svůj vlastní adresní rozsah a být do školní infrastruktury připojena Routerem. Netechnicky řečeno, Router spojuje dvě sítě a přenáší mezi nimi data. Router se podstatně liší od Switchu, který spojuje počítače v místní síti. Rozdílné funkce Routerů a Switchů si lze představit jako Switchu coby silnice spojující všechna města ve státě a Routery coby hraniční přechody spojující různé země.<sup>13</sup> Řízení přístupu předpokládá realizaci tak zvaného HotSpotu. HotSpot má v souvislosti s problematikou počítačových sítí hned několik významů. Obecně se tak označuje místo, kde se k síti připojuje větší množství uživatelů a kde je možné řídit jejich přístup.

Z hlediska projekce by se na první pohled zdálo, že bude nutné vybudovat hned dvě bezdrátové sítě se samostatným řízením přístupu. To by prakticky znamenalo dvojnásobný počet přístupových bodů, z nichž polovina by byla přístupná počítačům žáků a polovina by realizovala připojení provozních počítačů. Takové řešení by však bylo sice technologicky nejjednodušší, ale značně by se prodražilo z hlediska množství potřebného materiálu, vyžadovalo by ve většině případů značné rozšíření infrastruktury a v konečném pohledu by vyžadovalo celkem obtížnou správu. Při projekci jsem tedy začal studovat možnosti implementace přístupových bodů, které by umožňovaly na jediném zařízení vytvoření tak zvaných virtuálních sítí na bezdrátové technologii. Takové přístupové body skutečně na trhu nacházíme. Jistě nebude překvapením, že nejčastěji implementovaným řešením je RouterBoard od společnosti MikroTik. RouterBoard doplněný o mikro PCI WiFi kartu umožní konfiguraci několika virtuálních sítí a propojením na Radius Server správu uživatelů podle jejich příslušnosti do žákovské nebo provozní sítě. Takovému technicky elegantnímu řešení brání pouze fakt, že RouterBoard doplněný WiFi kartou vychází cenově přes 1800,- Kč, takže při odhadu použití 10 přístupových bodů umístěných na různých místech budovy se dostáváme k částkám vylučující toto řešení pro finanční náročnost.

---

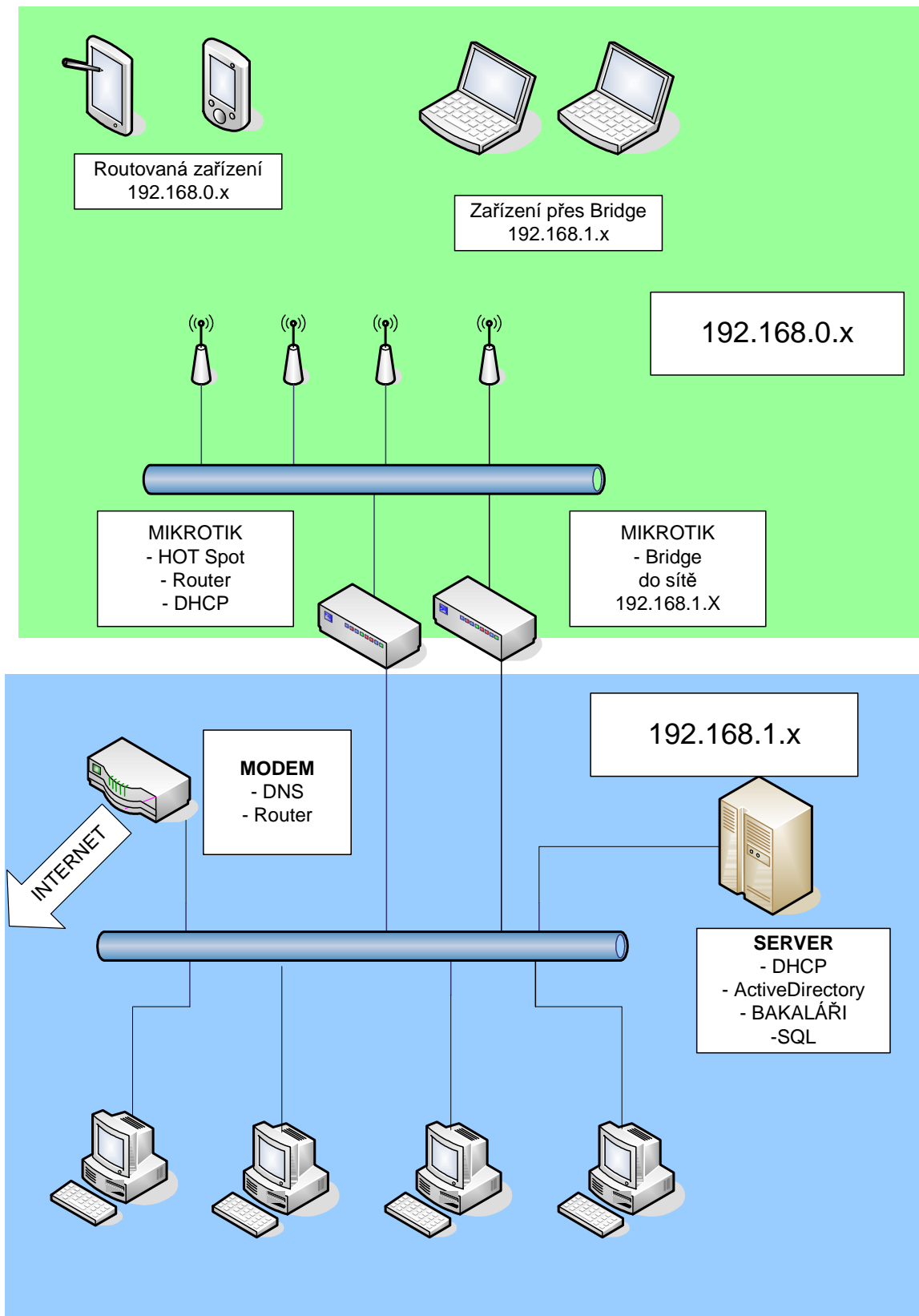
<sup>13</sup> Manual:BGP Case Studies. MIKROTIK MANUAL COPYRIGHT MIKROTIK 2008. BGP Case Studies [online]. modified on 14 April 2010 [cit. 2012-03-17]. Dostupné z: [http://wiki.mikrotik.com/wiki/Manual:BGP\\_Case\\_Studies](http://wiki.mikrotik.com/wiki/Manual:BGP_Case_Studies)



*Možnost nastavení virtuální bezdrátové sítě na platformě MikroTik*

Finální řešení se nabídlo ve chvíli, kdy z výchozích podmínek předpokládáme již existující bezdrátovou síť. Ta je v modelovém případě nedostačující z hlediska rozsahu pokrytí budovy signálem, způsobem zabezpečení a absencí individuálního řízení přístupu. Je realizována nejjednoduššími dostupnými technologiemi na trhu, určenými převážně pro domácí použití a možnosti jakékoliv konfigurace jsou značně omezené. Přesto si představme variantu, kdy je tato síť dobudována do požadovaného rozsahu, zbavena veškerého zabezpečení a oddělena od školní infrastruktury. Každý z přístupových bodů je nakonfigurován do již popsánoho módu Bridge a všechny přístupové body spojeny do jediného Switchu. Vzniká tak síť, která je z pohledu linkové vrstvy zcela totožná se sítí, kde se počítače pospojují bez jakéhokoliv řízení do Switchu strukturovanou kabeláží. Nastává prostor pro aplikaci aktivních členů, které určí konkrétní realizované spojení, respektive uživatele, tomu přiřadí adresu příslušné sítě, pro kterou je oprávněn a připojí jej. Podle typu uživatele (provozní počítač nebo student) si příslušná virtuální síť vyžádá autentifikaci.

Toto řešení nám umožní sestavit infrastrukturu z doslova stokorunových technologií a maximálně využít již používané části.



*Schématické znázornění projekčního záměru*

Předpokládána je tedy realizace měřením podloženého počtu přístupových bodů s nastaveným společným SSID a zbavených jakéhokoliv zabezpečení přístupu. Tyto přístupové body budou spojeny Switchem do společné sítě. Tuto síť budou se stávající infrastrukturou propojovat RouterBoard, který podle identifikace na základě fyzické adresy buď v případě provozních počítačů umožní spojení se školním serverem, načtení adresy přidělené tamtéž instalovaného DHCP serveru, nebo v případě žákovského počítače přesměrování na DHCP server v RouterBoardu, přidělení adresy z adresního rozsahu žákovské sítě a následné odkázání na HotSpot přihlašovací webovou stránku, vyžadující zadání individuálního uživatelského jména a hesla. To umožní studentovi přístup ke školnímu Routeru a následně k internetu.

Takový přístup snižuje požadavky na použitou technologii přístupových bodů. U těch předpokládáme jen tu nejzákladnější funkčnost a hlavním parametrem se tak stává cena. Z ekonomického i instalačního hlediska však bude velice výhodné, pokud zvolíme přístupové body disponující technologií PoE. PoE (Power over Ethernet) je napájení po datovém síťovém kabelu, bez nutnosti přivést napájecí napětí k přístroji dalším samostatným kabelem. Napájení po ethernetu se začalo výrazně prosazovat s nástupem internetové telefonie - VoIP. Dosavadní analogové nebo digitální (ISDN) telefony jsou co do napájení velmi nenáročné a vystačí obvykle s jedním párem vodičů zajišťujících jak komunikaci tak i napájení. VoIP má své nesporné výhody, ale napájení přístrojů — IP telefonů zvláštním kabelem bylo jednou ze zřejmých a závažných nevýhod. Běžné síťové přepínače neposkytovaly na svých rozhraních napájení pro připojené přístroje (PC, tiskárny, servery, datové terminály), předpokládal se vždy samostatný zdroj. Nástup VoIP na přelomu tisíciletí vyvolal tlak na řešení této otázky. Proto se kromě injektorů a pasivních napájecích panelů objevily i přepínače s napájecími porty. Jejich vyšší cena je vyrovnána zjednodušeným zapojením, možností centrální správy nyní nově i včetně napájení, úsporou kabelů atd., jak bylo uvedeno výše. Vyráběné PoE přepínače mají omezen celkový odebíraný výkon. Je to dáno výkonností jejich vestavěného zdroje. Platí běžná zásada, že vnitřní zdroj není dimenzován na součtový příkon přístrojů připojených na všechny porty přepínače současně, ale dovoluje napájet přibližně polovinu a často ještě méně.

Některé přepínače mají přímo označená rozhraní, kde je PoE a zbytek portů je nenapájecích.<sup>14</sup>



*PoE injektor*

Při použití PoE napájení se také vyhneme nutnosti zásahu do místní elektroinstalace a přispějeme k celkové bezpečnosti a modularitě řešení. Umístění přístupových bodů bude zcela nezávislé na stávající elektroinstalaci a obejdeme se tak bez případných kompromisů při umístování a použití ve školním prostředí zcela nevhodných prodlužovacích kabelů. Zároveň tak přístupové body nebudou jako elektrická zařízení napájená nízkým stejnosměrným napětím podléhat vyhlášce ZP 65/1965 Sb. § 133, odst. 1, písm. m o periodických revizích (pro školské instituce závazné).

Vzhledem k obrovské šíři trhu a neustálým změnám uvádím jen jako příklad ultra levný a pro účel projektu zcela dostačující přístupový bod Zcomax WA-2204A. Ten lze doporučit jak z hlediska ceny, tak robustním elektrotechnickým provedením, neboť z dlouholeté praxe pozoruji obrovskou odolnost tohoto výrobku proti zničení přepětím v datové síti, ke kterému dochází pravidelně při letních bouřkách. Kromě možnosti PoE napájení disponuje tento výrobek všemi potřebnými funkcemi a za cenu nepřesahující 500,- Kč jej lze jen doporučit.

---

<sup>14</sup> Power over Ethernet. In: *Wikipedie: Otevřená encyklopedie* [online]. 1.1. 20. 1. 2012 v 07:58. [cit. 2012-02-23]. Dostupné z: [http://cs.wikipedia.org/wiki/Power\\_over\\_Ethernet](http://cs.wikipedia.org/wiki/Power_over_Ethernet)



*Instalovaný Zcomax WA-2204A*

### **6.3. Měření**

Základním předpokladem úspěšné realizace je projekční část s návrhem optimálního pokrytí. Projekt musí zohledňovat použité technologie, stavební dispozice budovy a stávající stav infrastruktury. To vše včetně znalostí použitelných pásem nám umožňuje vytvořit hypotetický model pokrytí a umístění přístupových bodů. Je však nutné poznamenat, že před samotnou realizací je nutné úroveň signálu exaktně změřit a ověřit tak, že výsledná realizace bude splňovat požadavky pro provoz.

Pro modelování bezdrátového přenosu jsou určující nejen druh spoje (mobilní spoj, stálý spoj...) a vlastnosti přenosového prostředí, ale i typ a umístění antén. Pro popis pokrytí signálem existují dvě možnosti: úroveň signálu lze popsat jako intenzita elektrického pole v daném místě nebo jako výkonová úroveň přijatá referenční anténou s jednotkovým ziskem (0dB) .

V souvislosti v technologií WiFi se nejčastěji setkáme s šířením signálu v zastavené oblasti (zástavbě). Charakter šíření signálu, tj. i přístup k jeho modelování, je určen především okolním prostředím a umístěním pevné základnové antény. Tyto dva parametry jsou určeny zejména typem buňky. Z tohoto hlediska rozeznáváme

- **makrobunky:** pevná anténa je umístěná nad úrovní střech zástavby, poloměr buňky 1 – 30km
- **mikrobuňky:** pevná anténa je pod úrovní okolních střech zástavby, poloměr mikrobunky typicky 100 – 1000m
- **pikobunky:** pevná anténa je umístěna ve více či méně uzavřeném interiéru (například uvnitř školní budovy, v nákupní hale, apod.), rozměry buňky dosahují řádově desítek metru.

Vedle charakteru buňky lze modely šíření též dělit podle charakteru výpočtu na

- **empirické:** většinou jednoduché, aproximativní vztahy pro daný typ prostředí, ověřené přímo na místě pokusným měřením, kde jsou parametry založeny na statistické analýze naměřených dat
- **deterministické:** teoretické modelování na fyzikálním základe šíření vlny pro idealizovaný nebo více či méně zjednodušený popis daného prostředí (stavební konstrukce, materiál zástavby, apod.)
- **semi-empirické (semi-deterministické):** kombinace empirické a deterministické metody
- **stochastické:** na základě vstupních parametrů je náhodně generován průběh signálu pro simulaci přenosového kanálu, když obvykle není přímá vazba na geometrii přenosového prostředí a umístění antén

V praxi jsou díky své nenáročnosti na výpočetní prostředky, čas, specializovaný software a vstupní data nejpoužívanější modely empirické.<sup>15</sup>

### 6.3.1. Realizace měření

Měření bylo nutné provést empiricky z důvodů popsaných výše. Budova modelové školy je stavebně velice různorodá, setkáme se zde s plnými cihlovými zdmi, ale i s příčkami z itongu. Celá jedna část školy je moderní přístavbou s

---

<sup>15</sup> Pechac P.: Šíření vln v zástavbe. Nakladatelství BEN, Praha, 2005. 108str. ISBN 80-7300-186-1.

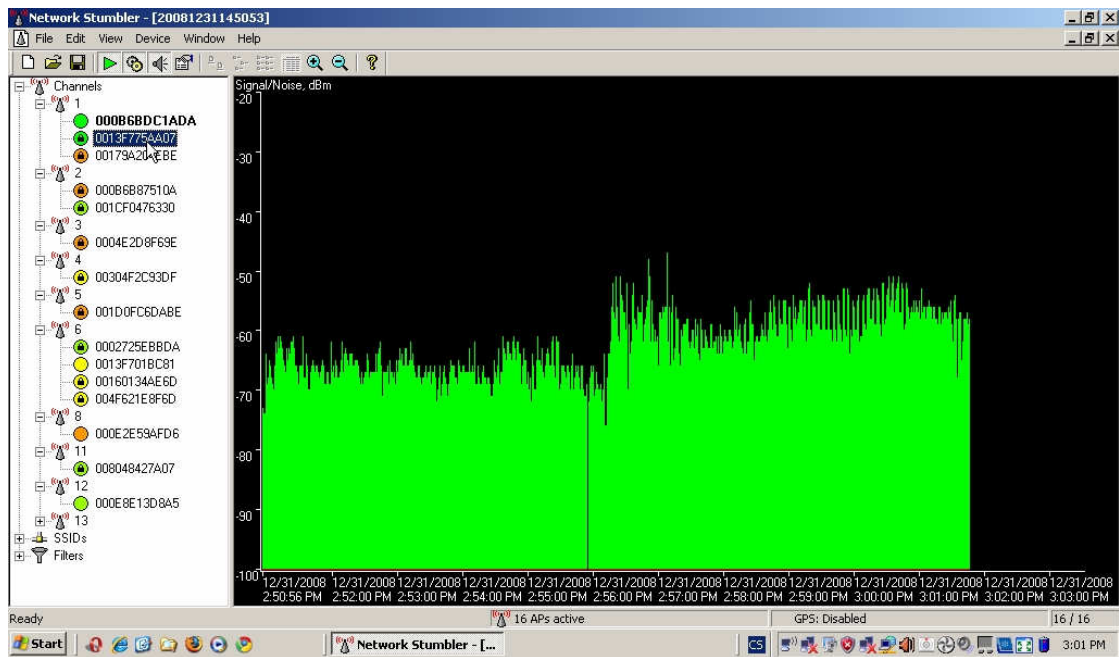


porotermových bloků. Jakákoliv simulace šíření signálu by tedy v takovémto případě byla náročná na technickou přípravu (naplnění simulačního software příslušnými daty) a mohla by se značně lišit od skutečnosti.

Postupoval jsem tedy tak, že jsem modelový vysílač WiFi signálu umisťoval do předem vytipovaných umístění a následně prováděl měření útlumu signálu v jednotlivých učebnách. Výsledky měření jsem zaznamenával do stavebního plánu budovy, takže nakonec vznikla průnikem jednotlivých měření mapa optimálního pokrytí signálem.

Legendárním programem jako stvořeným pro účel takového měření je Network Stumbler. Jedná se o univerzální freewarový nástroj pro monitoring bezdrátových sítí a mimo jiné síly jejich signálu, respektive poměru signál/šum. Přehledné zobrazování v podobě sloupcového grafu závislosti síly signálu (signál/šum [dB]) na čase umožňuje přehledné zobrazení kolísání signálu v různých místech učebny a umožňuje tak zcela optimální vyladění umístění vysílače. Pro případné zájemce o měření signálu tímto software však musím s politováním konstatovat, že nejsou podporovány síťové karty s čipovou sadou BroadCom, která je v poslední době na mobilních zařízeních v majoritě. Řešením může být USB WiFi adaptér, nebo podporovaný externí Access Point.

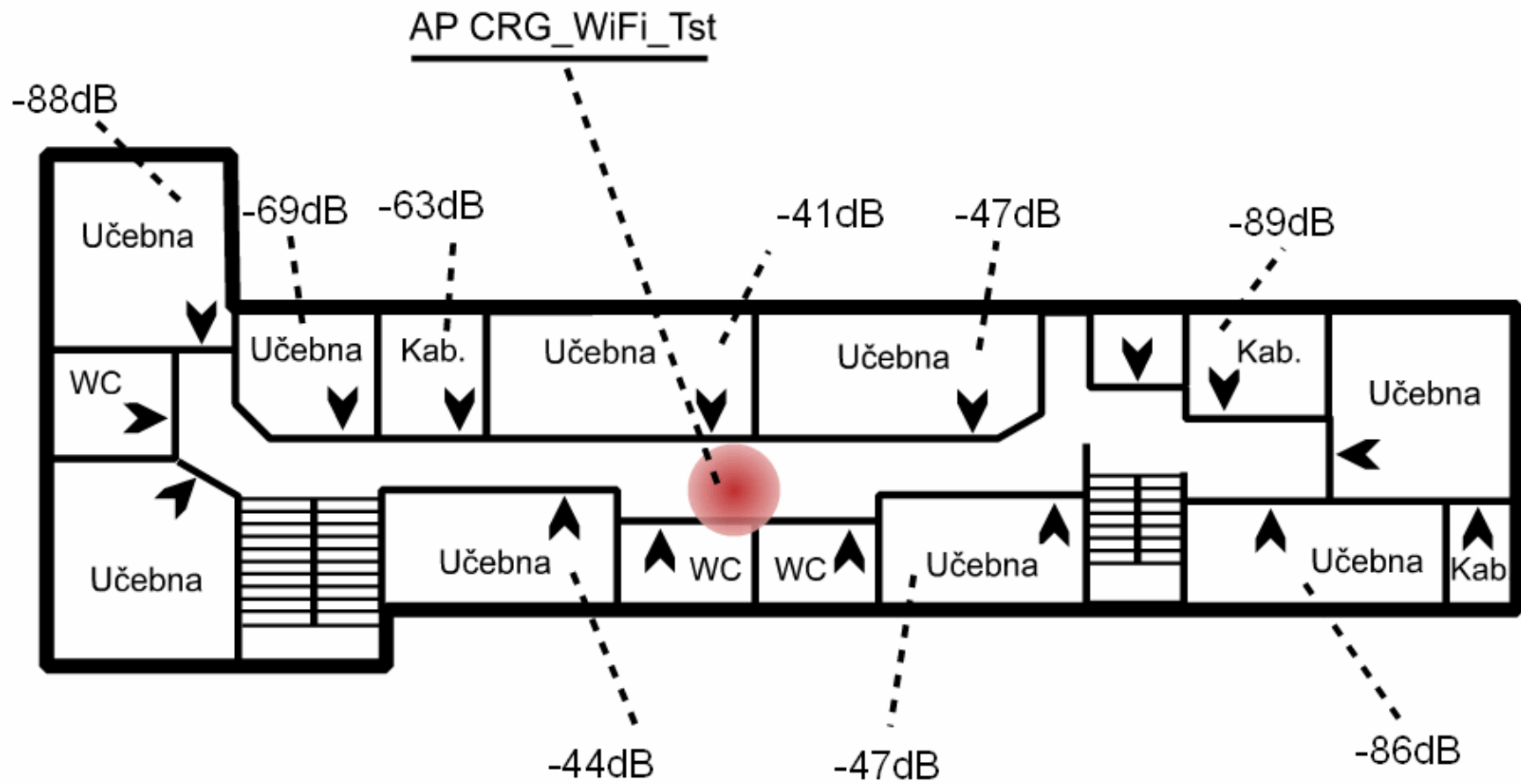
Pro jistotu stability spojení a zabezpečení optimální přenosové rychlosti jsem stanovil jakousi hranici  $-75\text{dB}$  poměru signál/šum při příjmu na běžný notebook. Při této úrovni signálu se dá předpokládat optimální přenosová rychlost i stabilita připojení i pro mobilní zařízení, jejichž anténa nemá tak velký zisk jako anténa integrovaná v notebooku. Tato hodnota, kterou jsem stanovil, je přísnější, než je vžitá praxe. Zde se předpokládá, že  $-85\text{dB}$  "je dost pro všechny".



*Network Stumbler - graf závislosti signál/šum na čase*



*Měření úrovně signálu v učebně*



*Příklad měření při modelovém umístění AP na jednom podlaží budovy ČRG*

## 6.4. Frekvenční pásmo

Jedním aspektů je i volba odpovídajícího frekvenčního pásma. Wi-Fi 2,4 GHz 802.11b je bezdrátová technologie pracující v přímém rozprostřeném spektru DSSS (Direct Sequence Spread Spectrum) s teoretickou přenosovou rychlostí 11 Mb/s u normy IEEE 802.11b a OFDM (Orthogonal Frequency Division Multiplexing) ortogonální multiplex s dělením kmitočtů pro 802.11g s teoretickou přenosovou rychlostí až 54 Mb/s. K dispozici je 38 frekvenčních kanálů, pro běžné použití je vyhrazeno pouze kanálů 14. V Česku v bezlicenčním pásmu pro bezdrátovou komunikaci pak 13 kanálů. Pásmo 5 GHz, technicky 802.11a, existuje od roku 1999. V České republice jeho plné nasazení prováděla celá řada omezení až do roku 2006.<sup>16</sup> Technologii provází celá řada vylepšení, vyšší směrovost antén i regulace výkonu. Pásmo je rozděleno, definováno a specifikováno pro Česko (resp. Evropu) v rozsahu 5,470GHz~5,725GHz to jest 11 nepřekrývajících se kanálů.

Přes jednoznačně vyšší přenosové rychlosti je třeba podotknout, že standard 802.11a není v současné době běžně podporován koncovými uživatelskými zařízeními a je pro účel budování otevřené školní sítě prakticky vyloučen. V použití ve vnitřních prostorách je třeba také vzít v potaz, že frekvence elektromagnetické vlny přímo ovlivňuje její chování v prostoru s překážkami, kterým školní budova bezesporu je. Pro ilustraci uvádím srovnání mezi pásmem 2,4GHz a pásmem 5GHz:

---

<sup>16</sup> *airdump.cz* [online]. 2009 [cit. 2011-06-18]. Teorie WiFi sítí. Dostupné z WWW: <<http://wiki.airdump.cz>>.

<b>specifika frekvence 2,4 GHz:</b>	<b>specifika frekvence 5 GHz:</b>
<ul style="list-style-type: none"> <li>- délka vlny je cca 12,5 cm,</li> <li>- vlnění je z 95% pohlcováno vodou a organickými látkami (listnaté stromy, dřevo), vlnění se zcela odrazí od jakékoliv překážky větší než délka vlny</li> </ul>	<ul style="list-style-type: none"> <li>- délka vlny je cca 6 cm, vlnění je méně pohlcováno vodou</li> <li>- zcela se odrazí od jakékoliv překážky větší než délka vlny je náchylnější na přímou viditelnost více než vlnění na 2,4 GHz</li> </ul>

Četnost odrazů je značným determinantem pro přenosovou rychlost. Normované rychlosti jsou totiž jakýmsi vytouženým cílem, který je ovlivňován řadou faktorů, počínaje zarušením pásma z okolních vysílačů a konče útlumem signálu průchodem stavebních konstrukcí. Každé zařízení pak uvádí katalogové hodnoty pro úroveň signálu, která zaručuje přenos dat rychlostí, kterou umožňuje pásmo, a dále pak úroveň, pod kterou datový přenos není vůbec garantován, nebo není možný. Následující vztah vám umožní převod hodnot udávaných v miliwattech na decibely:

$$P_{dB} = 10 \log(P_W \cdot 1000)$$

V oblasti přenosů elektromagnetické vlny je rozměr udávaný v decibelech v celku běžný a praktický. O významu tohoto počínání vzhledem k potřebám projekce WiFi sítě se budu dále zmiňovat v kapitole o měření signálu v konkrétním projekčním případě.

## **6.5. Řízení provozu bezdrátové sítě**

Předpokladem pro úspěšný a bezproblémový provoz školní sítě, tedy především její zákovské části, bude i vytvoření pravidel pro uživatele. Vzhledem k tomu, že každý uživatel má své přístupové údaje, je možné uživatele s těmito pravidly seznámit a vyžadovat jejich dodržování. Za nejzákladnější rizika ze strany dětských uživatelů lze označit:

### **6.5.1. Neúnosné zatížení připojení k internetu**

V současné době má většina škol stabilní širokopásmové připojení, které umožňuje jej poskytnout studentům pro běžné použití, tedy prohlížení webu, přístup k

mailu, chatu a ostatním komunikačním službám. Bohužel v reálném provozu se setkáváme s tím, že studenti využívají hromadně školní připojení ke stahování velkých souborů z internetu a dochází tak k následnému přetížení poskytovaného připojení. To vede k efektu zpomalení připojení a následným problémům, které se mohou projevit i v oficiální výuce nebo provozu IT služeb ve škole.

Projektované řešení obsahuje modul pro správu uživatelů dostupný správci přes webové rozhraní. V tomto modulu lze snadno a přehledně filtrovat uživatele podle množství přijatých a odeslaných dat. Následně lze jednoznačně určit tak zvané "stahovače" a přístup jim omezit nebo podmíněčně pozastavit.

<input type="checkbox"/>	▼ Username ▲	▼ Prepaid ▲	▼ Used ▲	Left	▼ Price ▲	▼ Download ▲	▼ Upload ▲
<input type="checkbox"/>	<a href="#">salcbl</a>	unlimited	1w:3d:14h:54m:33s	0s	0.00	124.0 GiB	6.3 GiB
<input type="checkbox"/>	<a href="#">troide</a>	unlimited	1w:16h:45m:35s	0s	0.00	37.7 GiB	6.4 GiB
<input type="checkbox"/>	<a href="#">tichzu</a>	unlimited	1w:2d:6h:44m:34s	0s	0.00	26.6 GiB	1899.0 MiB
<input type="checkbox"/>	<a href="#">hrouma</a>	unlimited	5d:4h:45m:45s	0s	0.00	19.4 GiB	775.6 MiB
<input type="checkbox"/>	<a href="#">hnizel</a>	unlimited	1w:2d:38m:53s	0s	0.00	18.5 GiB	617.3 MiB
<input type="checkbox"/>	<a href="#">drazda</a>	unlimited	1w:1d:14h:30m:36s	0s	0.00	17.9 GiB	737.7 MiB
<input type="checkbox"/>	<a href="#">belope</a>	unlimited	5d:11h:30m:8s	0s	0.00	15.9 GiB	542.1 MiB
<input type="checkbox"/>	<a href="#">halaji</a>	unlimited	4d:6h:25m:26s	0s	0.00	15.8 GiB	803.5 MiB
<input type="checkbox"/>	<a href="#">schaal</a>	unlimited	1w:4d:20h:2m:43s	0s	0.00	14.2 GiB	549.1 MiB
<input type="checkbox"/>	<a href="#">dupast</a>	unlimited	1w:1d:5h:34m:13s	0s	0.00	13.7 GiB	983.0 MiB
<input type="checkbox"/>	<a href="#">klimpa</a>	unlimited	6d:4h:14m:1s	0s	0.00	11.0 GiB	447.2 MiB
<input type="checkbox"/>	<a href="#">rousve</a>	unlimited	5d:16h:27m:7s	0s	0.00	9.9 GiB	511.3 MiB
<input type="checkbox"/>	<a href="#">afanbo</a>	unlimited	4d:3h:44m:2s	0s	0.00	9.1 GiB	363.4 MiB
<input type="checkbox"/>	<a href="#">pokofi</a>	unlimited	1w:17h:13m:39s	0s	0.00	8.8 GiB	443.9 MiB
<input type="checkbox"/>	<a href="#">janama</a>	unlimited	5d:18h:24m:50s	0s	0.00	8.2 GiB	341.9 MiB
<input type="checkbox"/>	<a href="#">hoffda</a>	unlimited	2d:22h:21m:23s	0s	0.00	7.2 GiB	234.5 MiB
<input type="checkbox"/>	<a href="#">sestij</a>	unlimited	1w:1d:22h:56m:20s	0s	0.00	7.2 GiB	618.4 MiB
<input type="checkbox"/>	<a href="#">kadlte</a>	unlimited	6d:13h:17m:23s	0s	0.00	6.9 GiB	750.4 MiB
<input type="checkbox"/>	<a href="#">pobopa</a>	unlimited	3d:22h:2m:55s	0s	0.00	6.9 GiB	447.3 MiB
<input type="checkbox"/>	<a href="#">uhliga</a>	unlimited	1w:23h:13m:3s	0s	0.00	6.5 GiB	575.5 MiB

1 2 3 4 5 6 7 8 >> (Total: 151) Per page: 20

Edit Generate Search

*Náhled do User Manageru s aplikovaným řazením podle množství stažených dat*

Řešení je pak na správci sítě nebo jiné pověřené osobě, která může podle statistických dat zjednat nápravu. Výše uvedená aplikace pro správu uživatelů umožní případně i omezení rychlosti připojení konkrétním studentům, což může být jeden z možných regulačních nástrojů.

The screenshot shows a web-based interface for editing a user. The 'Rate limits' section is highlighted with a red box, containing fields for RX and TX limits for Rate, Burst rate, Burst threshold, and Burst time. The 'Private Information' section is expanded, showing fields for IP Address, Pool Name, Group, and Address List. The 'Download limit', 'Upload limit', and 'Transfer limit' are all set to 0. The 'Uptime Limit' is set to 0s. The 'Priority' is set to 'not specified'. The 'Min rate' fields for RX and TX are empty. The 'Uptime Used' is 5d18h24m50s, 'Download Used' is 8.2 GiB, and 'Upload Used' is 341.9 MiB. The 'Add time' dropdown is set to 'no credits available'. The 'View report', 'Show Sessions', and 'Save' buttons are at the bottom.

*User Manager s možností omezení rychlosti stahování a odesílání dat*

## 6.5.2. Přístup k nevhodnému obsahu

Přístup k nevhodnému obsahu je často skloňovaná tématika související s každodenním používáním informačních technologií ve školském prostředí. Problematika je veskrze velice široká a odráží se v ní samozřejmě i fakt, že se nevhodné obsahy velice těžko efektivně identifikují pomocí automatických metod. Navržený systém samozřejmě mimo jiné umožňuje provoz v režimu tak zvané Walled

Garden (zahradka obehnaná zdí). Tato funkce definuje volně přístupné webové stránky. Na HotSpot aplikacích se většinou používá komerčně, kdy povoluje přístup ke komerčním stránkám (např. místních cestovních kanceláří nebo obchodních partnerů), a cíleně tak poskytne svým zákazníkům službu navíc. Ve školském prostředí by bylo tedy možné vyjmenovat povolený webový obsah.

Názory na takový přístup se ale značně rozcházejí. Podle mého názoru se jedná o vyloženě sisyfovskou práci, neboť ruku v ruce s vývojem technik pro omezení přístupu k určitému obsahu na internetu vznikají logicky techniky, jak se k němu dostat. Zároveň je faktem, že podobná omezení vzbuzují odpor ze strany uživatelů, tedy studentů, a vyvolávají emotivní diskuze o svobodě přístupu k informacím a filosofickému základu internetu jakožto svobodné síti. Ze zkušeností z praxe se domnívám, že účinnější než striktní represivní zákrok je vhodnější osvěta a výchova k odpovědnému přístupu v oblasti využívání informačních technologií.

V modelovém řešení je tato oblast postihnuta provozním řádem a pravidly pro užívání školní sítě. Z morálního hlediska se bráním jakémukoliv monitoringu osobní síťové komunikace, který by pravděpodobně mohl hraničit s porušením platných zákonů.

### **6.5.3. Neautorizovaný přístup**

Získání neautorizovaného přístupu přes HotSpot by bylo reálně možné pouze za cenu značně odborné technické manipulace s aktivním prvkem, ke které by bylo nutné získat fyzický přístup k technologii. Proto je vhodné ji umístit s ohledem na tuto skutečnost. Častěji dochází ke získání přístupových práv od jiných uživatelů zjištěním jejich hesel nebo extrakcí údajů přímo z počítače (uložená hesla, správci hesel a podobně). Riziko je značně zvýšeno i použitím "slabých" hesel. Neautorizovaný přístup ke školnímu připojení do internetu je relativně neškodný a těžko zneužitelný. Ostatní služby v síti předpokládají vlastní zabezpečení.

Vyvstává zde však opět myšlenka důležitosti osvěty týkající se odpovědnému přístupu k informačním technologiím a osobním údajům v elektronickém světě. Stále častěji docházím k přesvědčení, že tato oblast informační gramotnosti je napříč společnostmi polem neoraným a nesetým.



Z výše popsaných skutečností vyplývá, že v každé škole umožňující volný přístup žáků k internetu by měla na základě uvážlivé diskuse vzniknout pravidla, se kterými jsou uživatelé seznámeni, vnitřně je akceptují a jsou ochotni je dodržovat. Na modelové škole vznikl provozní řád obsažený v příloze.

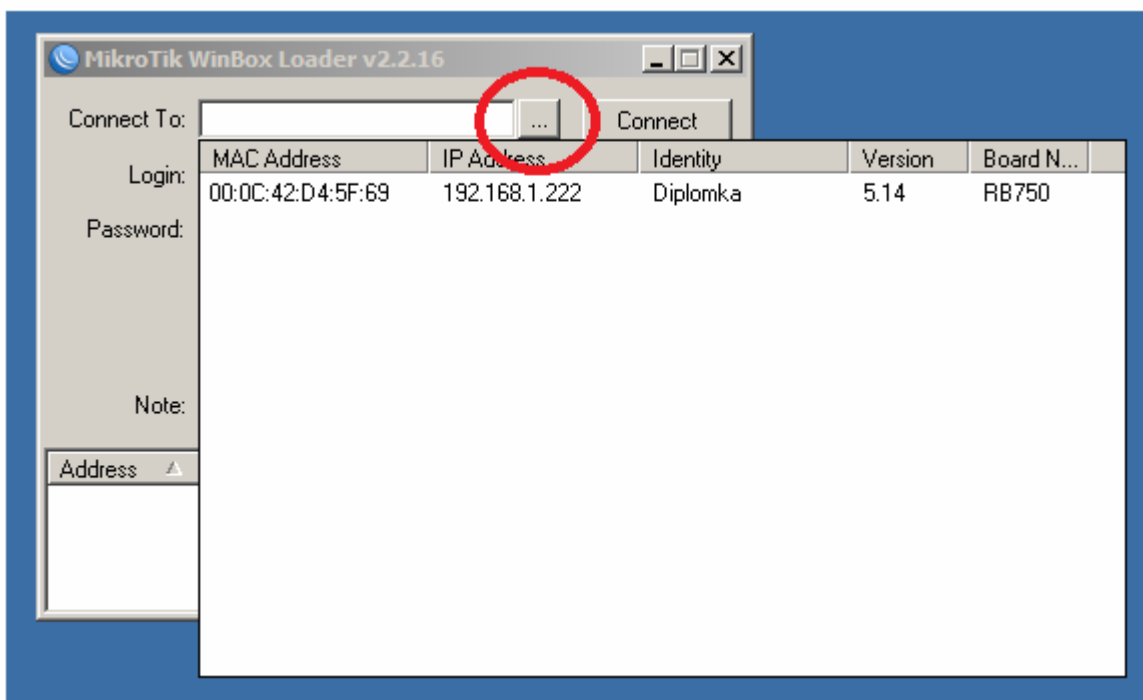
## **6.6. Konfigurace RouterBoardu Mikrotik**

Srdcem celého řešení, jak již bylo popsáno, se stává RouterBoard firmy Mikrotik. Ačkoliv je na trhu celá škála těchto zařízení, optimálním modelem pro nasazení v této aplikaci se jeví výrobek označený jako RouterBoard 750. Je výhodný z hlediska konstrukce, již předinstalované verze operačního systému a cenou. Přestože doporučuji nákup právě tohoto modelu, všechny skripty pro automatickou konfiguraci, které budou popsány, nejsou vázány právě na toto zařízení a je možné je aplikovat na libovolný hardware s operačním systémem Mikrotik. Správce, který se rozhodne popsané řešení realizovat, může jednoduše následovat popsané kroky a moduly, jejichž nastavovací skripty nalezne na přiloženém CD a ty přizpůsobí stávající infrastruktuře.

### **6.6.1. Prostředí WinBox**

Pro práci s RouterBoardem existuje uživatelsky příjemné a přehledné prostředí s názvem WinBox. Tato utilita je volně ke stažení na stránkách <http://www.mikrotik.com/download.html> a není třeba ji instalovat, takže ji může správce spustit třeba ze svého flash disku na libovolném počítači.

Po spuštění je třeba připojit WinBox k RouterBoardu, který nastavujeme. Výhodou je, že připojení je nezávislé na IP adrese počítače i RouterBoardu. Při kliknutí na tlačítko na konci řádky "Connect to" (viz obrázek dále) se síť automaticky skenuje a vyhledávají se dostupná, připojená zařízení s operačním systémem Mikrotik. Zvolením příslušné MAC adresy ve výčtu nalezených RouterBoardů se automaticky vyplní příslušná hodnota. Pole "Login" je třeba v základním nastavení dopsat hodnotou "admin" a heslo zůstává prázdné. Stisknutím tlačítka "Connect" se připojíte k RouterBoardu a můžete jej nastavovat.



*Připojení k RouterBoardu utilitou WinBox*

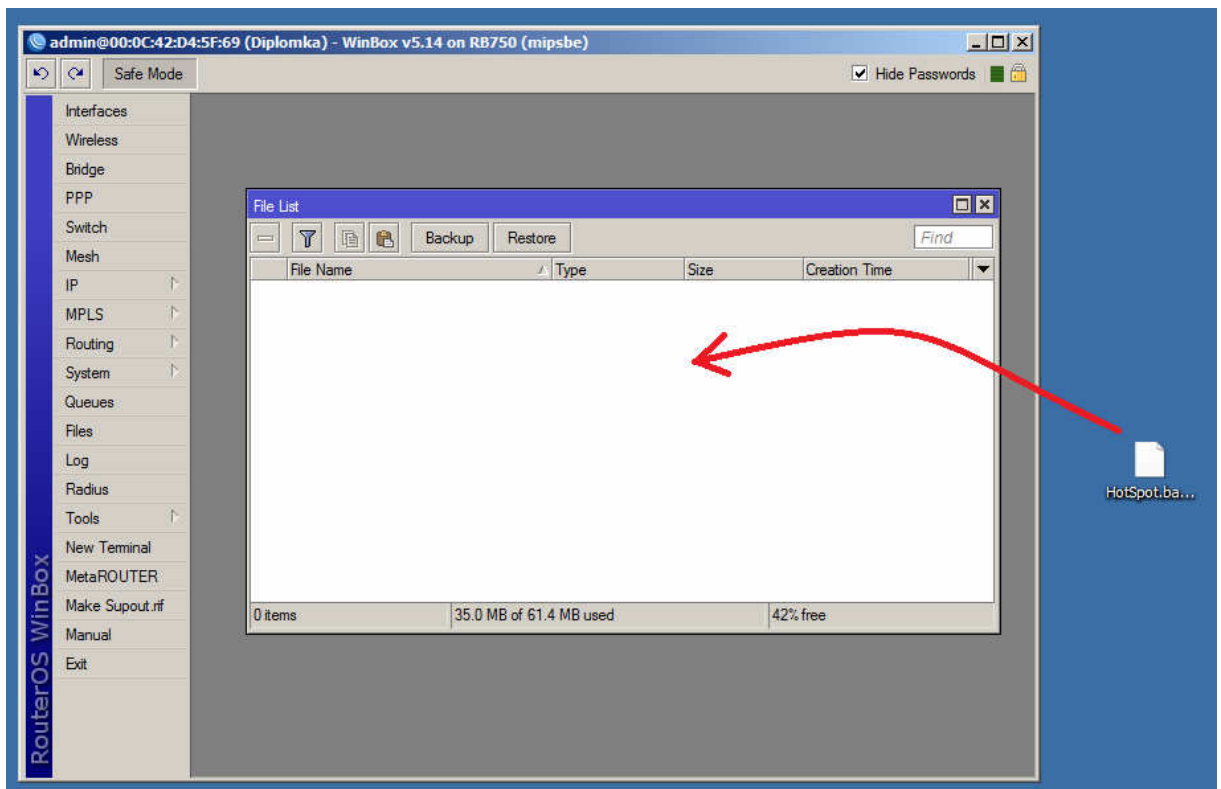
## 6.6.2. Nahrání konfiguračního skriptu

Příložené CD obsahuje celkem 3 soubory s konfiguračními skripty.

- **HotSpot.backup** - přidělí každému počítači IP adresu a po spuštění internetového prohlížeče ho vyzve k zadání přístupových údajů. Bez zadání těchto údajů nemá počítač přístup k žádným dalším síťovým službám. Tento skript zároveň obsahuje správce uživatelů dostupného přes internetový prohlížeč, pomocí něž správce povoluje, nebo ruší uživatelská konta pro přístup. Tento modul je v modelovém řešení použit jako přístupový bod žákovské sítě a vytváří nový adresní rozsah odlišný od adresního rozsahu školní sítě, který je routován k připojení do internetu.
- **Bridge&HotSpot.backup** - je kombinací obou předchozích skriptů. Jedná se o případ aplikace souběhu dvou virtuálních sítí na jednom WiFi připojení. Podle MAC adresy je počítač přes bridge propojen do školní sítě, je mu serverem přidělena adresa a dále je v modelovém řešení chápán jako počítač ve školní doméně. Pokud není jeho MAC adresa povolena, je automaticky přesměrován na stránku HotSpotu a je mu přidělena adresa žákovské sítě, což mu umožní po zadání jeho přístupových údajů přístup k internetu, ale ne do školní sítě a její domény.

- **Bribge.backup** - Tento skript je přiložen pro případ, že by systém byl instalován na RouterBoardy nižších tříd. Tam dochází k tomu, že se při připojení odpovídajícímu souběhu bridge a routeru zablokuje rozsah ARP tabulky a dochází k pádu aplikace. Řešením je použití dvou nezávislých RouterBoardů, kdy na jeden je aplikován skript Bridge.backup a na druhý HotSpot.backup. Bridge.backup umožní vyjmenovaným počítačům přístup do sítě bez zadávání dalších údajů. Tento modul je v modelovém řešení použit pro přístup školních počítačů do domény na školním serveru. Server pak také připojeným počítačům přiděluje IP adresy z vlastního DHCP rozsahu. Ostatním (nevyjmenovaným) počítačům přístup neumožňuje. Přístup není závislý na přihlášeném uživateli a jeho právech v síti, ale na MAC adrese počítače.

Je tedy třeba zvolit vhodný soubor se záložním skriptem. Jeho instalace je velice jednoduchá. V menu na levém okraji okna WinBoxu zvolte položku "Files" a do okna, které se objeví, přetáhněte soubor se zvoleným záložním skriptem (viz obrázek níže). Poté na soubor klikněte a zvolte tlačítko "Restore". Volbu potvrďte a po restartu RouterBoardu (může trvat až 2 minuty) je RouterBoard nakonfigurován na požadovaný modul.



*Kopírování záložního scriptu v prostředí WinBox*

K modulu HotSpot.backup a Bridge&HotSpot.backup je třeba ještě stejným způsobem přidat adresář Hotspot, který je rovněž součástí přiloženého CD.

### **6.6.3. Personalizace nastavení síťových rozhraní**

Všechny záložní skripty výše popsané obsahují nastavení IP adresních rozsahů, které nemusí odpovídat nastavení sítě při aplikaci do libovolného síťového prostředí. Je tedy nutné je přizpůsobit požadovanému stavu. Pomocí výše zmíněné aplikace WinBox je po připojení k RouterBoardu možné IP adresy jednotlivých použitých portů měnit pod položkou menu "IP". Podřízená položka "Adresses" obsahuje nastavení IP adres všech použitých portů. V případě aplikace konfiguračního skriptu HotSpot.backup, nebo Bridge&HotSpot.backup je třeba konfigurovat i DHCP server ve stejnojmenné položce menu "IP" a přidělovaný adresní rozsah v položce "Pool".

Základní nastavení ve zmíněných skriptech:

	Port 1	Port 2	Port 4	Port 5
<b>Hotspot</b>	WAN 192.168.1.201	- 192.168.0.1 DHCP 192.168.0.2 - 192.168.0.255	x	x
<b>Bridge&amp;HotSpot</b>	WAN 192.168.1.201	- 192.168.0.1 DHCP 192.168.0.2 - 192.168.0.255	WAN 192.168.1.202	LAN 192.168.10.10
<b>Bridge</b>	x	x	WAN 192.168.1.202	LAN 192.168.10.10

#### 6.6.4. Personalizace přihlašovací stránky HotSpotu

Předpokládá se i přizpůsobení stránky, která se uživateli objeví při spuštění internetového prohlížeče. Na přiloženém CD se nalézají adresář "HotSpot" obsahující řadu souborů, z nichž podstatným je soubor "login.html". Tento soubor se zobrazuje uživateli při spuštění internetového prohlížeče pro registraci k přístupu k síťovým službám. Nejjednodušší možností, jak tuto stránku upravit, aby odpovídala požadavkům příslušného školského zařízení, je editace zobrazovaného obrázku, který se nachází v adresáři "hotspot\img" pod názvem login.jpg. Takovou úpravu zvládne pravděpodobně každý průměrně informačně gramotný uživatel. Adresář "hotspot" však obsahuje i soubory obsahující xml a kaskádových stylů, takže zkušenému programátorovi nic nebrání stránku přepracovat do zcela originální podoby.



*Náhled přihlašovací stránky v podobě uložené na CD*

## 6.7. Bezdrátová infrastruktura

V rámci realizace projektu se předpokládá výstavba, případně doplnění bezdrátové části sítě. Na modelové škole, kde je systém pokusně aplikován již před zahájením realizace, částečné pokrytí bezdrátovou sítí existovalo (viz 3.1.1. Stávající infrastruktura - výchozí podmínky). Bylo tedy třeba podle projekčního návrhu síť doplnit a připravit na připojení aktivního řídicího prvku - RouterBoardu Mikrotik.

Konfiguraci realizujeme u přístupových bodů přes rozhraní webového prohlížeče. Konfigurační prostředí se samozřejmě bude lišit podle použitých typů přístupových bodů, ale obecně lze říci, že podle přiložených manuálů ji zvládne i průměrně informačně gramotný uživatel. Z nastavení, kterým musíme věnovat pozornost, bych zmínil rozhodně heslo do konfiguračního menu. Nechat jej v podobě továrního nastavení by bylo zcela nevhodné, protože je téměř jisté, že se zvědavý student pokusí zjistit, jak to celé funguje. Dále je výhodné u všech přístupových bodů nastavit pevné IP adresy a zapsat si, kde jsou fyzicky umístěny. V praxi se často stává, že je třeba některé části infrastruktury vyměnit, diagnostikovat výpadky v pokrytí a podobně. Pokud známe adresu konkrétního přístupového bodu, je diagnostika především u větších sítí o mnoho lehčí.

Zcela výjimečnou pozornost bude třeba věnovat nastavení SSID přístupových bodů. Pokud nastavíme na všech přístupových bodech stejné SSID, vyřešíme problematiku tak zvaného roamingu. Předpokládáme totiž, že se během dne bude uživatel připojený k síti pohybovat po budově a je vhodné, aby se automaticky připojoval k síti bez ohledu na to, který přístupový bod pokrývá jeho okamžité umístění. Pokud všechny přístupové body budou poskytovat stejné SSID, připojované zařízení si vybere nejsilnější signál, respektive kanál s příslušným SSID a nejsilnějším signálem.

The screenshot shows the ZCOMAX WLAN Access Point configuration interface. On the left is a navigation menu with 'Site contents' including Status, Setup Wizard, Operation Mode, Wireless, TCP/IP Settings, Firewall, VPN Setting, Management, and Logout. The main content area is titled 'WLAN Access Point' and 'Broadband Router Status'. Below the title, it states: 'This page shows the current status and some basic settings of the device.' The status is presented in a table with green headers for each section.

System	
Uptime	0day:0h:14m:1s
Firmware Version	v1.4.7.P
Wireless Configuration	
Mode	AP+WDS
Band	2.4 GHz (B+G)
SSID	CRG_WiFi
Channel Number	4
Encryption	Disabled(AP), Disabled(WDS)
BSSID	00:02:72:8c:c7:17
Associated Clients	6
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.10.222
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Disabled
MAC Address	00:02:72:8c:c7:17

*Náhled konfiguračního menu použitého přístupového bodu*

V konfiguraci přístupových bodů je z dalších konfiguračních možností třeba dodržet:

- DHCP server - zakázat. Souběh více DHCP serverů v síti by byl problematický. Přidělování adres bude řídit RouterBoard nebo server v pevné infrastruktuře.
- Zabezpečení - vypnout. Používání WEP, WPA a podobně není třeba, protože přístup bude řízen centrálně.

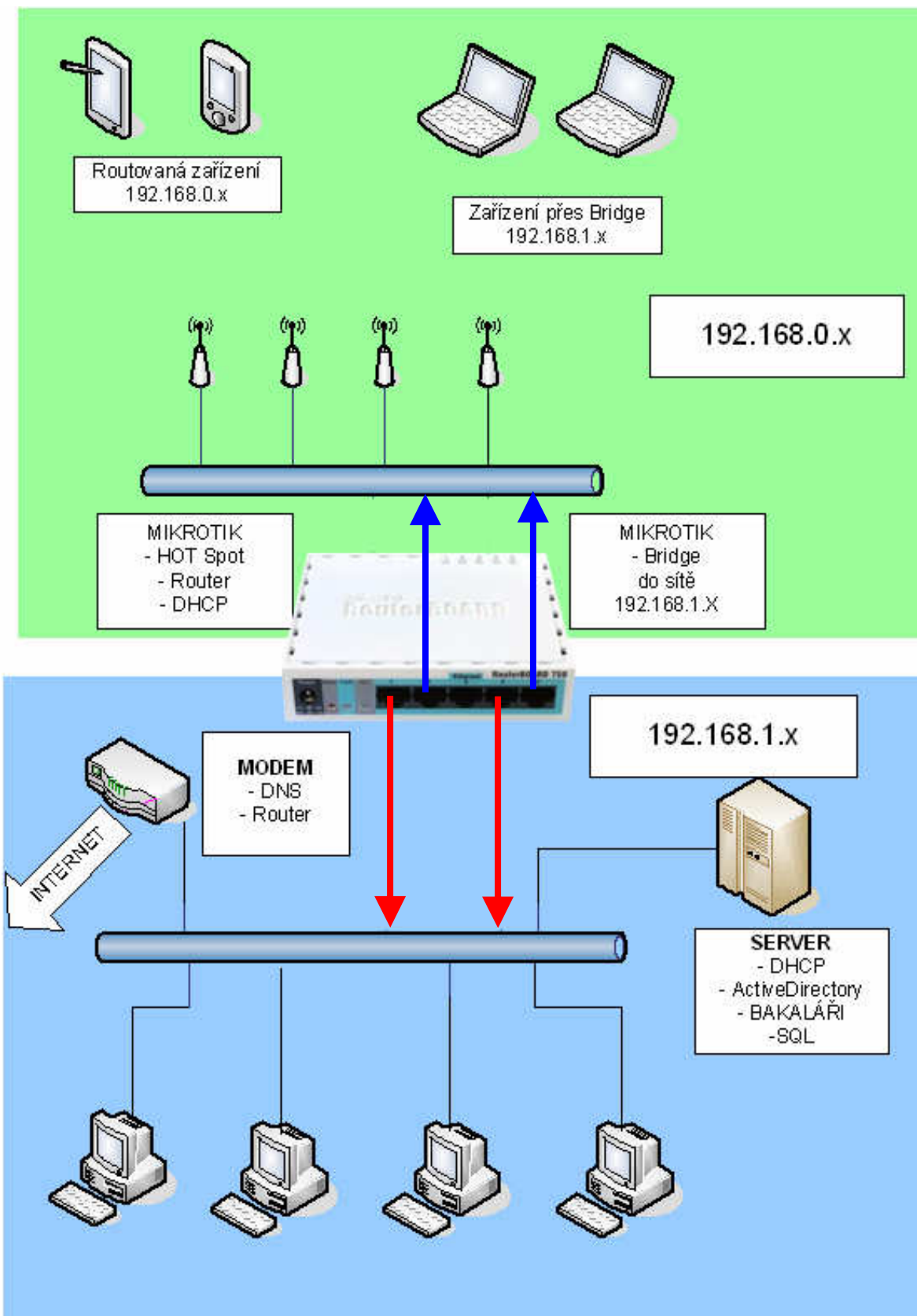
- Mód přístupu - bridge. V případě routování na úrovni přístupového bodu by vznikl problém s připojením provozních počítačů do domény.

## 6.8. Připojení bezdrátové části sítě

Propojení pevné části sítě a vytvoření bezdrátové infrastruktury se realizuje v závislosti na zvoleném konfiguračním skriptu podle následujícího schématu, které je zároveň skutečným stavem na modelové škole. Celá bezdrátová síť, to znamená všechny přístupové body, jsou spojeny switchem do společné sítě. Tu od pevné části infrastruktury odděluje RouterBoard, který je v tomto případě konfigurován jako HotSpot a bridge (konfigurační skript Bridge&HotSpot.backup). Zde jsou porty 1 a 4 použity jako porty WAN, kterou zde reprezentuje pevná síť (červené šipky na obrázku viz dále). Porty 2 a 4 jsou použity jako připojení sítě LAN, za kterou v tomto případě považujeme bezdrátovou infrastrukturu.

V případě volby konfiguračního skriptu HotSpot.backup je port 4 a 5 nekonfigurován a nepřipojuje se. Obdobně i v případě aplikace konfiguračního skriptu Bridge.backup jsou konfigurovány pouze porty 4 a 5, takže porty 1 a 2 se nepřipojují.





*Schématické znázornění skutečného propojení*

## 6.9. Administrace uživatelů

Správa uživatelů, kteří budou mít přístup do sítě, se liší podle typu přístupu k systému. Jak již bylo dříve popsáno, rozlišujeme uživatele

- s přístupem do pevné sítě a školní domény, tak zvané provozní uživatele (pedagogy a školní počítače s bezdrátovým připojením)
- s přístupem ke školnímu připojení do sítě internet, tedy soukromá zařízení žáků (notebooky, tablety, telefony)
- uživatele bez povoleného přístupu

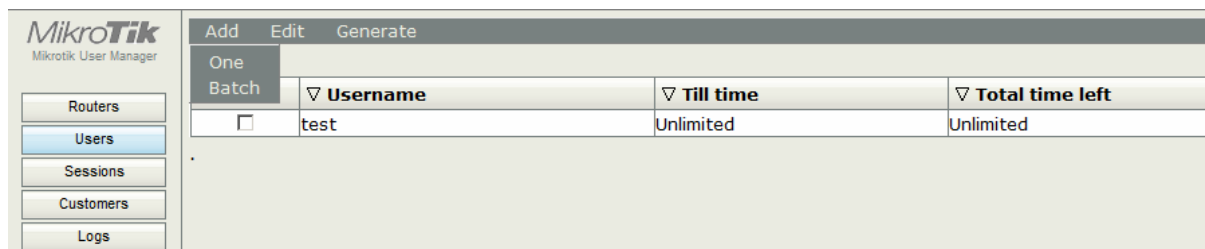
Výčet provozních uživatelů je konfigurován přes popsanou aplikaci WinBox formou výčtu fyzických adres příslušných počítačů. Tento filtr nalezneme po připojení k RouterBoardu v menu Bridge a kartě Filters. V základní konfiguraci jsou již jako příklad tři pravidla. Pro každý počítač, který bude mít automaticky přístup do školní sítě, potažmo do její domény, je třeba první dvě pravidla označená jako "Příklad 1" kopírovat a změnit v nich požadovanou MAC adresu. Pravým tlačítkem myši stisknutým na nově vytvořené položce se zpřístupní možnost "Coment", kterou je vhodné vyplnit názvem počítače (nebo jménem vlastníka) pro lepší orientaci. Po dokončení zadání potřebných pravidel je nezbytné přetáhnout položku s pravidlem nazvaným "LAN to WAN zakázané" přetáhnout na poslední místo ve výčtu pravidel. Tím je určeno, které počítače se mohou dostávat do sítě přes bridge a žádat pevnou síť (respektive server) o poskytnutí dalších síťových služeb.

#	Chain	Interfaces...	Interfaces...	Src. MAC Address...	Dst. MAC Address...	MAC Prot...	Bytes	Pac
0	forward	ether5	ether4	00:21:5D:17:E7:4A			0	
1	input	ether2-h...		00:21:5D:17:E7:4A			0	
2	forward	ether5	ether4				0	

### *Filtry pro přístup provozních počítačů*

Všechny ostatní počítače jsou směrovány na přihlašovací stránku HotSpotu. Zde je uživatel žádán o zadání přístupového jména a hesla. Jejich správa je realizována

přes webové rozhraní dostupné na adrese konfigurované na portu 1. Při základním nastavením konfiguračních skriptů bude tedy dostupný správce uživatelů na adrese 192.168.1.222/userman. Po jejím zadání se v prohlížeči spouští aplikace na všeobecnou správu uživatelů, kde lze uživatele přidávat, odebírat i editovat jejich údaje. Pro velké školy, kde správce požaduje zřízení velkého počtu uživatelů, je zde možné uživatele i hromadně generovat a následně jejich přístupové údaje vytisknout.



The screenshot shows the MikroTik User Manager interface. On the left is a sidebar with navigation buttons: Routers, Users (highlighted), Sessions, Customers, and Logs. The main area has a header with 'Add', 'Edit', and 'Generate' buttons. Below the header is a table with columns: Username, Till time, and Total time left. A single user entry is visible with Username 'test', Till time 'Unlimited', and Total time left 'Unlimited'.

	Username	Till time	Total time left
<input type="checkbox"/>	test	Unlimited	Unlimited

*Náhled do správce uživatelů HotSpotu*

## 6.10. Rozpočet na realizaci modelového řešení

Jedním ze zadávacích kritérií je samozřejmě cena. Jak již bylo popsáno v teoretické části, jsou finance obecným problémem, který determinuje používání a rozvoj bezdrátových technologií na školách. V případě modelové realizace byl použit materiál dle rozpisu, který je součástí přílohy.

Celková cena v případě modelového řešení byla 8191,- Kč. Je však třeba zdůraznit, že se jedná pouze o cenu materiálu a není zde promítnuta cena za instalační práce. V tomto případě byla veškerá práce provedena bez nároku na honorář, protože se jednalo o pokusnou, modelovou instalaci. Při instalačních pracích bylo vystavěno asi 65 metrů nové kabelové trasy pomocí elektroinstalačních lišt. Částečně byly využity kabelové trasy stávající infrastruktury. Během instalace se spotřebovalo přes 250 metrů strukturované kabeláže. Celá výstavba v tomto rozsahu zabrala asi 20 pracovních hodin. K tomuto faktu je třeba přihlídnout v případě, že by instalace byla prováděna na komerční bázi.

Při odhadu reálných cen v oblasti elektroinstalačních prací lze předpokládat, že v případě realizace komerční firmou by se cena celkové dodávky navýšila zhruba o 10000,- Kč. Jedná se však pouze o hrubý odhad, protože komerční realizace je otázkou nabídky a tvorba nabídkové ceny je úzce specifická pro každého dodavatele. S jistotou

Ize ale tvrdit, že částka 35000,- Kč zmíněná v úvodu praktické části by měla být bez problémů dodržena při podobném rozsahu potřebného rozšíření infrastruktury.

## 7. Závěr

Cílem první části diplomové práce byl teoretický výzkum, který se zabýval vybavením školských zařízení síťovými technologiemi, umožňujícími připojení uživatelů k internetu a dalším síťovým službám na školách používaných. Proběhlý dotazníkový výzkum i doprovodné pohovory na téma předmětu výzkumu statisticky potvrdily data poskytnutá Českou školní inspekcí v rámci šetření proběhlého v letech 2009 až 2010. Výsledky hovoří o potřebě zvýšení dostupnosti informačních technologií mezi pedagogy. Z koncepcí vedení škol je patrné, že těžiště segmentu nově pořizované výpočetní techniky se znatelně přesouvá směrem k mobilní technice. Nesporné výhody notebooků jsou do značné míry determinovány možností připojením k bezdrátové síťové infrastruktuře, která, jak vyplývá z výzkumu, na školách zcela chybí, je nedostatečně rozšířená nebo nevhodně a těžkopádně zabezpečená. Rozšíření bezdrátových technologií brání především fakt, že systémy umožňující připojení počítačů podle požadavků specifických pro toto prostředí nejsou běžně na trhu. V konečném řešení se jedná buď o kompromis ze strany požadavků, nebo zakázkové řešení, které by bylo finančně náročné.

Z vlastního výzkumu pak vyšlo modelové zadání, které požaduje od realizovaného systému provoz žákovské a provozní sítě, přičemž provozní síť umožňuje připojení školním počítačům s přímým přístupem do domény školní sítě. Jedním ze základních parametrů tak zvané žákovské sítě, která umožní žákům připojit jejich technologie k internetu prostřednictvím školní interní sítě, je personifikované řízení. Je tedy požadováno zřízení uživatelských účtů každému žákovi a možnost jeho omezení v případě potřeby.

V rámci těchto požadavků byly podrobeny zkoumání různé technologie, které nabízí trh. Jejich vlastnosti byly posuzovány podle kritérií, která vplynula nejen z možnosti nasazení na takovou aplikaci, ale též z hlediska modularity a nezávislosti na platformě stávající infrastruktury ve školském zařízení. V opačném případě by se jednalo opět o zakázkové řešení bez možnosti nasazení na libovolném školském

zařízení. Jako univerzální a na platformě nezávislé řešení byl vybrán operační systém MikroTik v kombinaci se stejnojmenným RouterBoardem, který se objevuje na trhu a v poslední době získává stále více na popularitě v celé řadě síťových aplikací.

Druhým cílem diplomové práce je konkrétní návrh infrastruktury rozšíření vnitřní školní sítě o bezdrátovou část splňující požadavky vzešlé z první teoretické části. Na vybraném RouterBoardu od firmy MikroTik bylo nakonfigurováno rozhraní mezi pevnou a bezdrátovou infrastrukturou, které umožňuje podle zařazení konkrétního počítače do provozní nebo studentské části jeho adresné připojení. Rovněž byl na studentskou část aplikován správce uživatelů dostupný přes webové rozhraní, který umožní hromadnou správu studentských účtů pověřenému pracovníkovi, který tím pádem nemusí být nijak zvlášť zdatný informatik. Celkové sestavení bylo nasazeno na modelové škole a byl na něm spuštěn chod provozní sítě a zároveň bylo umožněno studentům zřizování uživatelských účtů pro přístup k internetu prostřednictvím vnitřní školní sítě.

Během uvedení systému do provozu byl sestaven i provozní řád, který postihuje aspekty bezpečného přístupu k žákovské síti a po odsouhlasení vedením modelové školy se stal doplňkem školního řádu. Tento materiál je součástí příloh diplomové práce.

Z kompletní konfigurace RouterBoardu byl vytvořen kompletní konfigurační skript, který je obsažen na CD přiloženém k diplomové práci. Jeho aplikací na RouterBoard je možné vytvoření obdobného rozhraní, které je poté možné v případě zájmu aplikovat i na jiných školách. Celá praktická část diplomové práce postihuje problematiku projekce a výstavby takovéto infrastruktury, takže zájemcům o obdobnou nebo podobnou realizaci poskytne jakýsi návod.

Cíle diplomové práce byly naplněny, což prokazuje fakt, že v práci navržený systém je nasazen v nezměněné podobě na dvou školách v Českých Budějovicích a na dvou dalších školních zařízeních existuje v podobě bez možnosti přístupu žáků. Vznikla tak alternativa, která je pro správce školních sítí, ICT koordinátory i vedení škol možným řešením při snaze o masivní zpřístupnění informačních technologií pedagogickým pracovníkům, případně i studentům. Zároveň, jak dokládá kapitola zabývající se rozpočtovou otázkou a finanční náročností projektu, se jedná o systém dostupný z běžných rozpočtových zdrojů.

## 8. Literatura

- [1] Cíle a vize >>Vzdělání 21<< [online]. 2010, 1, [cit. 2011-02-14]. Dostupný z WWW: <<http://www.vzdelani21.cz/cile-a-vize/>>.
- [2] Cisco Systems, Inc. Cisco BBSM Hotspot 1.0: User Guide. In: Www.cisco.com [online]. [cit. 2012-03-03]. Dostupné z: [http://www.cisco.com/en/US/docs/net\\_mgmt/cisco\\_building\\_broadband\\_service\\_manager/hotspot/1.0/user/guide/hs10\\_pf.html](http://www.cisco.com/en/US/docs/net_mgmt/cisco_building_broadband_service_manager/hotspot/1.0/user/guide/hs10_pf.html)
- [3] Český statistický úřad, SRNSKÁ, Zuzana. Co říkají výzkumy a statistiky o vybavenosti ICT na základních školách. Online, 2010, s. 3.
- [4] Česká školní inspekce. Úroveň ICT v základních školách v ČR \*online. c2010, poslední revize 20. 11. Dostupné z: <<http://www.csicr.cz/cz/85156-uroven-ict-v-zakladnich-skolach-v-cr>>.
- [5] GNU's Not Unix!: Radius. GNU's Not Unix! [online]. [cit. 2012-03-17]. Dostupné z: <http://www.gnu.org/software/radius/>
- [6] What is router OS: OS MikroTik. In: [Http://www.mikrotik.com/pdf/what\\_is\\_routeros.pdf](http://www.mikrotik.com/pdf/what_is_routeros.pdf) [online]. [cit. 2012-02-18]. Dostupné z: [http://www.mikrotik.com/pdf/what\\_is\\_routeros.pdf](http://www.mikrotik.com/pdf/what_is_routeros.pdf)
- [7] ŠTRAUCH, Adam. Mikrotik: Seznámení s Wi-Fi krabičkou. In: Www.root.cz [online]. 7. 11. 2008 [cit. 2012-02-18]. Dostupné z: <http://www.root.cz/clanky/mikrotik-seznameni-s-wi-fi-krabickou/>
- [8] airdump.cz [online]. 2009 [cit. 2011-06-18]. Teorie WiFi sítí. Dostupné z WWW: <<http://wiki.airdump.cz>>.
- [9] Power over Ethernet. In: Wikipedie: Otevřená encyklopedie [online]. 1.1. 20. 1. 2012 v 07:58. [cit. 2012-02-23]. Dostupné z: [http://cs.wikipedia.org/wiki/Power\\_over\\_Ethernet](http://cs.wikipedia.org/wiki/Power_over_Ethernet)
- [10] Pechac P.: Šíření vln v zástavbe. Nakladatelství BEN, Praha, 2005. 108str. ISBN 80-7300-186-1.

## 9. Přílohy

### 9.1. Průvodní dopis k dotazníkovému šetření

*Vážení kolegové,*

*dovoluji si oslovit vás s prosbou o pomoc při šetření zaměřeném na stav a požadavky v oblasti IT infrastruktury ve školských zařízeních. Data z tohoto výzkumu budou použita jako teoretický podklad k mé diplomové práci. Výzkum obsahuje jednak jednoduchý dotazník, který mapuje stávající stav IT infrastruktury na škole, dále pak část, ve které zkoumám používání, plány a požadavky. Vzhledem k tomu, že druhou část nelze objektivně shrnout do dotazníku, požádám vás o krátký rozhovor, z něhož vypracuji souhrnný výstup.*

*Samozřejmě chápu, že máte množství pracovních povinností. Výsledkem tohoto šetření a vaší spolupráce by však měla být práce, která nejen teoreticky rozebírá aspekty používání IT technologií na bázi bezdrátového připojení, ale i úplná projektová dokumentace modelového řešení, které lze implementovat ve školském prostředí s přihlédnutím k jeho specifikům. Výsledky práce Vám budou na požádání poskytnuty s možností konzultace realizace navrženého modelového řešení.*

*S pozdravem Petr Syrovátka - student JU PF*

## 9.2. Dotazník statistického šetření

Dotazník k vybavenosti školy informačními technologiemi			
Škola:			
Počet žáků:		Počet tříd:	
Počet pedagogů:			
PC žákovských:		PC pro pedagogy:	
z toho v LAN:		z toho v LAN:	
z toho notebooků:		z toho notebooků:	
Připojení k internetu	Ano/Ne	Technologie:	
		Rychlost:	
Počet serverů:		OS serverů:	
Server spravuje:			
Lokální síť	Ano/Ne	Rychlost sítě:	
Bezdrátová síť	Ano/Ne	Přístup žáků	Ano/Ne
		Přístup pedagogů	Ano/Ne
Jakým způsobem je řízen přístup uživatelů k bezdrátové síti?			



## **9.3. Pravidla užívání bezdrátové sítě Českého reálného gymnázia s. r. o. CRG\_WiFi**

### **1. Oprávnění k užívání CRG\_WiFi**

- Každý zaměstnanec i student Českého reálného gymnázia s.r.o. (dále ČRG) může požádat o zřízení uživatelského účtu pro přístup do sítě CRG\_WiFi.
- Při vytvoření účtu a zvolení hesla se uživatel podpisem zavazuje dodržovat pravidla pro užívání bezdrátové sítě (viz níže).

### **2. Pravidla k užívání CRG\_WiFi**

- Uživatel se zavazuje získané přístupové údaje držet v tajnosti a využívat je výhradně pro svou potřebu. V případě ztráty přihlašovacích údajů nebo jejich prozrazení je uživatel povinen kontaktovat administrátora pro jejich změnu.
- Uživatel bude používat přístup do sítě výhradně k přístupu ke sdíleným informačním službám (zejména internetu). Nebude se pokoušet získat přístup do chráněných částí sítě ani do datových úložišť jiných uživatelů připojených do sítě.
- Uživatel chrání síť i ostatní uživatele před hrozbou viru nebo jiné formě elektronického útoku zejména užíváním aktualizovaného antivirového systému a instalací pravidelných bezpečnostních aktualizací. V případě zjištění virové infekce na počítači je uživatel povinen se od sítě odpojit až do odstranění problému.
- Při užívání internetu se uživatelé zdrží návštěv stránek s nevhodným nebo nelegálním obsahem. Rovněž je zakázáno v rámci sítě stahovat velké objemy dat, zdržovat se na streamových serverech (on-line sledování videa) a jinak zatěžovat sdílené připojení.
- Uživatel je seznámen se skutečností, že provoz sítě je monitorován a že v důsledku chování směřujícímu k omezení provozu sítě nebo při porušení výše uvedených nařízení může být zbaven práva síť užívat.

### **3. Zřízení uživatelského účtu**

- Pro zřízení uživatelského účtu prosím kontaktujte správce sítě.
- V budově ČRG naleznete v dostupných WiFi sítích nezabezpečenou síť CRG\_WiFi.
- Po připojení k této síti a spuštění internetového prohlížeče budete vyzváni systémem k zadání uživatelského jména a hesla.
- Správným jménem a heslem zpřístupníte připojení.
- Správcem systému je p. Syrovátka.

## 6.4 Cenová kalkulace

### Rozpis materiálu pro realizaci systému řízeného přístupu k bezdrátové síti na Českém reálném gymnáziu s. r. o. Pražská 54a, České Budějovice

Tabulka následujícího materiálu obsahuje veškeré součásti instalace, které bude třeba nakoupit pro kompletní realizaci projektového zadání. Ceny jsou závazné po dobu jednoho měsíce od podání nabídky a jsou uvedeny včetně daně z přidané hodnoty. Záruční doba je 24 měsíců od předání realizovaného projektového řešení.

Název zboží	cena za kus	kusů	cena za položku
AP Z-Comax WA-2204A-TX	542,00 Kč	7	3 794,00 Kč
MikroTik RB 750	840,00 Kč	1	840,00 Kč
TP-LINK TL-SF1024D 24x10/100	1 452,00 Kč	1	1 452,00 Kč
UTP kat. 5e, 305m BELDEN	1 120,00 Kč	1	1 120,00 Kč
Instalační lišta 2cm x 2cm x 2m	21,00 Kč	35	735,00 Kč
Spotřební materiál	250,00 Kč	1	250,00 Kč

**CELKEM 8 191,00 Kč**

