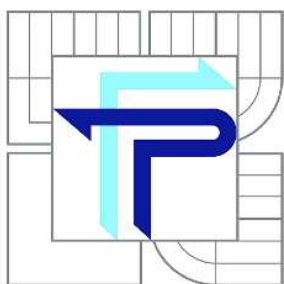


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ  
BRNO UNIVERSITY OF TECHNOLOGY



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

## NÁVRH BEZDRÁTOVÉ SÍTĚ PRO SOŠ PODYJÍ

CONCEPT OF WIRELESS NETWORK FOR SOŠ PODYJÍ

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE

AUTHOR

PETR TRUHLÁŘ

VEDOUcí PRÁCE

SUPERVISOR

doc. Ing. MILOŠ KOCH, CSc.

BRNO 2010

## ZADÁNÍ BAKALÁŘSKÉ PRÁCE

**Truhlář Petr**

---

Manažerská informatika (6209R021)

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

**Návrh bezdrátové sítě pro SOŠ Podyjí**

v anglickém jazyce:

**Concept of Wireless Network for SOŠ Podyjí**

Pokyny pro vypracování:

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

Seznam odborné literatury:

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

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

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2009/2010.

L.S.

---

Ing. Jiří Kříž, Ph.D.  
Ředitel ústavu

---

doc. RNDr. Anna Putnová, Ph.D., MBA

V Brně, dne 26.05.2010

## **Anotace závěrečné práce**

Pro svoji práci jsem si vybral návrh bezdrátové sítě, která bude v praxi aplikována na SOŠ Podyjí. V této práci se budu zabývat výběrem vhodného standardu bezdrátové sítě a jeho využití. Teoretická část mé práce se bude zabývat problematikou bezdrátových sítí a jejich zabezpečení. V praktické části bude vybráno nejvhodnější řešení z uvedených standardů, zabezpečení a zařízení s ohledem na pořizovací cenu.

## **Anotation**

For my paper I have chosen project of a wireless network, which will be actually applied at SOS Podyji. In my paper I will deal with selection of a suitable concept of the wireless network and the functional use of the concept. In a theoretical part of my paper I will engage in wireless networks in general and in security of wireless networks. In a practical part of my paper I will select the most convenient solution, combining the chosen concept, security features and networking devices. I will select the networking devices with regard to their price.

## **Klíčová slova**

Wi-Fi, IEEE 802.11, LAN, WAN, WEP, WPA, WPA2, bezpečnost bezdrátových sítí, topologie sítí, UTP, STP

## **Keywords**

Wi-Fi, IEEE 802.11, LAN, WAN, WEP, WPA, WPA2, security of wireless networks, network topology, UTP, STP

## **Bibliografická citace práce**

TRUHLAR, P. *Návrh bezdrátové sítě pro Střední odbornou školu Podyjí*. Brno: VUT v Brně, Fakulta podnikatelská, 2010. 52 s. Vedoucí práce: doc. Ing. Miloš Koch, CSc.

## **Čestné prohlášení**

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 10. května 2010

-----  
Petr Truhlář

## **Poděkování**

Tímto bych rád poděkoval panu doc. Ing. Miloši Kochovi, CSc., vedoucímu této bakalářské práce, za jeho užitečné rady a přínosnou metodickou pomoc, které jsem využil při zpracování bakalářské práce.

# OBSAH

ÚVOD .....	10
CÍLE PRÁCE .....	11
1 TEORETICKÁ VÝCHODISKA PRÁCE .....	12
1.1 Topologie sítí .....	12
1.1.1 BUS (sběrnice) .....	12
1.1.2 RING (kruh) .....	12
1.1.3 STAR (hvězda) .....	12
1.1.4 Hybridní sítě .....	13
1.2 Síťová propojení .....	13
1.2.1 Metalické spoje .....	13
1.2.2 Optické spoje .....	14
1.2.3 Bezdrátové spoje .....	15
1.3 ISO/OSI model .....	15
1.3.1 Fyzická vrstva .....	16
1.3.2 Linková vrstva .....	16
1.3.3 Síťová vrstva .....	17
1.3.4 Transportní vrstva .....	18
1.3.5 Relační vrstva .....	18
1.3.6 Prezentační vrstva .....	18
1.3.7 Aplikační vrstva .....	19
1.4 Propojovací zařízení .....	19
1.4.1 Repeater (opakovač) .....	19
1.4.2 Hub (rozbočovač) .....	19
1.4.3 Switch (přepínač) .....	20
1.4.4 Router (směrovač) .....	20
1.4.5 Brána (gate) .....	20
1.4.6 Most (bridge) .....	20
1.5 Přístupové metody .....	21
1.5.1 CSMA/CD – metoda náhodného přístupu (drátový ethernet) .....	21
1.5.2 CSMA/CA - Vícenásobný přístup s předcházením kolizí (bezdrátový ethernet) .....	21
1.6 Typy bezdrátových sítí .....	21
1.6.1 Ad-hoc sítě .....	22
1.6.2 Infrastrukturní sítě .....	22
1.7 Přenosové techniky standardů 802.11 .....	23
1.7.1 DSSS .....	23
1.7.2 FHSS .....	23
1.7.3 OFDM .....	24
1.7.4 MIMO .....	24
1.8 Rodina standardů IEEE 802.11 .....	24
1.8.1 IEEE 802.11 .....	24
1.8.2 IEEE 802.11a .....	25
1.8.3 IEEE 802.11b .....	25

1.8.4	IEEE 802.11g.....	25
1.8.5	IEEE 802.11n.....	26
1.9	Bezpečnostní mechanizmy Wi-Fi sítě .....	26
1.9.1	SSID.....	26
1.9.2	Filtrování MAC adres .....	27
1.9.3	WEP.....	27
1.9.4	WPA.....	28
1.9.5	WPA2.....	29
1.9.6	IEEE 802.1X.....	29
1.10	Možné útoky na bezdrátové sítě .....	31
1.10.1	Zjištění SSID.....	31
1.10.2	Změna MAC adres.....	31
1.10.3	Man in the Middle.....	32
2	ANALÝZA PROBLÉMU .....	33
2.1	Charakteristika organizace.....	33
2.1.1	Základní údaje.....	33
2.1.2	Historie.....	33
2.2	Analýza budovy .....	34
2.2.1	První patro budovy školy.....	34
2.2.2	Druhé patro budovy školy.....	35
2.3	Analýza rychlosti připojení k internetu .....	37
2.4	Analýza požadavků potencionálních uživatelů.....	37
3	VLASTNÍ NÁVRH ŘEŠENÍ .....	39
3.1	Fáze realizace projektu .....	39
3.2	Výběr přístupových bodů.....	40
3.3	Výběr antén.....	41
3.4	Rozmístění antén a přístupových bodů .....	41
3.4.1	Návrh vylepšení signálu.....	43
3.5	Zapojení přístupových bodů do páteřní sítě.....	44
3.6	Úpravy elektrické instalace pro napájení přístupových bodů .....	44
3.7	Nastavení přístupových bodů.....	44
3.8	Ekonomické zhodnocení.....	45
	ZÁVĚR .....	46
	POUŽITÉ ZDROJE.....	47
	Knížní zdroje.....	47
	Elektronické zdroje .....	47
	SEZNAM POUŽITÝCH ZKRATEK.....	49
	SEZNAM OBRÁZKŮ.....	50
	SEZNAM TABULEK .....	50
	SEZNAM PŘÍLOH.....	50

## ÚVOD

Vzhledem k dnešnímu trendu stále se rozvíjejících multimediálních technologií je absence bezdrátové sítě na střední škole velkým nedostatkem. V dřívější době, kdy se na této škole vyučovaly pouze obory jako jsou „Pozemní stavitelství“ a „Veřejnoprávní činnost“, nebylo zapotřebí tolik počítačů s internetovým připojením. S nástupem nového oboru „Správce informačních systémů“ bylo za potřebí rozšíření počítačových učeben a počítačových sítí. Jednalo se o metalické infrastruktury, které byly provedeny externí firmou. V čase, kdy tyto sítě byly budovány, se ceny bezdrátových řešení pohybovaly příliš vysoko a jejich zabezpečení bylo nedostačující. V současné době většina studentů vlastní přenosné počítače, které v sobě mají zabudovány drátové a bezdrátové síťové karty. Tito studenti by rádi své počítače používali nejenom doma, ale také ve škole. Vzhledem k nutnosti používání internetu pro vyhledávání potřebných informací ke studiu, bylo vedení požádáno o vytvoření přístupu k internetu. Představa rozvádění kabelů do každé učebny a vytváření dostatečného počtu přípojek je finančně nákladná a zbytečná. Z tohoto důvodu se škola rozhodla pro vytvoření bezdrátové sítě v celé budově a já jsem se tohoto úkolu ujal. V této práci se budu tímto úkolem zabývat a hledat nejvhodnější řešení pro tuto situaci. Jelikož se bude jednat o návrh bezdrátové sítě, budu se snažit zvolit co nejvhodnější standard řešení a také se budu zabývat zabezpečením této sítě. I když se bude jednat pouze o školní síť, budu se snažit vytvořit co nejvýhodnější podmínky zabezpečení pro bezpečnost potenciálních uživatelů.

V teoretické části mé práce se budu zabývat jak strukturovanou kabeláží, topologií sítí, propojovacími zařízeními, tak bezdrátovými technologiemi a jejich zabezpečením. Jelikož počítačové sítě jsou velice rozsáhlou kapitolou, budu se zabývat pouze okruhy, které budou použity v praktické části.

V praktické části mé práce se budu věnovat samotnému návrhu této sítě, bude vypracováno nejvhodnější řešení s konečnou kalkulací, která budou posléze poskytnuta a předvedena firmě „Střední odborná škola Podyjí s.r.o.“.

## CÍLE PRÁCE

- Informovat o základních termínech používaných při Wi-Fi problematikách.
- Rozvést otázku zabezpečení sítí.
- Navrhnout řešení komplikací.
- Přejít k tvorbě vlastní sítě, jejího využití a prakticky ukázat problémy, na které běžně narážíme.

# 1 TEORETICKÁ VÝCHODISKA PRÁCE

## 1.1 Topologie sítí

Síťové topologie jsou popisy toho, jak jsou počítače rozmístěné, jak jsou zapojené a hovoří o dalších prvcích sítě, jako jsou například centrální prvky. V následujících podkapitolách jsem čerpal z [24].

### 1.1.1 BUS (sběrnice)

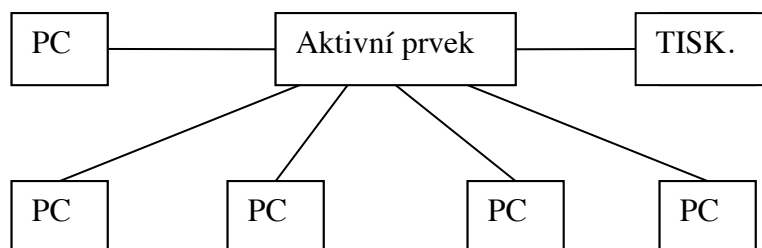
Jedná se o staříčkový princip propojení počítačů koaxiálními kabely za použití tzv. páteřního vedení. Jelikož tato topologie nebude použita v této práci, nebudu se k ní již dále vracet.

### 1.1.2 RING (kruh)

V této topologii je vytvořen skutečný fyzický kruh a funguje tak, že vysílající část jednoho uzlu je zapojena do přijímací části uzlu následujícího. Tato topologie není součástí této práce, nebudu se jí již dále zabývat.

### 1.1.3 STAR (hvězda)

Tento druh topologie patří mezi nejrozsáhlejší a nejpoblárnější v této době. Její princip je založen na tom, že za pomoci nějakého centrálního prvku (aktivní prvek), nejčastěji to bývá rozbočovač (hub), přepínač (switch) a nebo směrovač (router), jsou do všech ostatních uzlů přenášeny signály po samostatných kabelech. Veškerá komunikace prochází centrálním prvkem a při výpadku nějakého z kabelů, nedochází ke kolizi celé sítě, tak jak to bývalo u předchozích technologií.



**Obrázek 1.1:** Topologie STAR (hvězda), zdroj vlastní

### 1.1.4 Hybridní síť

Toto jsou kombinace výše zmíněných topologií. Mohou se zde vyskytnout spojení jako jsou například STAR-BUS nebo STAR-RING.

## 1.2 Síťová propojení

Sledované vlastnosti:

- Přenos signálu (elektromagnetické vlnění, viditelné světlo, infračervené světlo atd.)
- Pořizovací náklady
- Instalační požadavky
- Šířka pásma (bandwidth) – kapacita média
- Útlum (attenuation) – slábnutí signálu
- Vzájemné ovlivňování (NEXT)
- Elektromagnetická interference (EMI)

Následné informace v podkapitolách byli čerpány z [2].

### 1.2.1 Metalické spoje

Jsou obecně levnější než jiné způsoby. Bohužel mívají problémy s odolností vůči elektromagnetickému záření.

### 1.2.1.1 Koaxiální kabely

I když se jedná o velmi levné řešení, kde není zapotřebí žádné propojovací zařízení, je tato technologie již minulostí. Skoro nikde se již nepoužívá vzhledem k její maximální rychlosti 40 Mb/s.

### 1.2.1.2 Kroucená dvojlinka

Jelikož je moje práce zaměřena na vytvoření bezdrátové sítě, kroucenou dvojlinku budu používat pouze pro zasílání přístupových bodů (o nichž se budu zmiňovat v dalších kapitolách). V tomto případě se zaměřím na nestíněnou kroucenou dvojlinku (UTP). V dnešní nabídce máme k dispozici osm kategorií metalických kabelů. Pro naše využití jsou vhodné pouze kabely kategorie pět a vyšší. Bude ovšem záležet, na tom, jaký přístupový bod bude v mém návrhu použit a jaké bude mít specifikace. Na základě těchto specifikací bude zvolena vyhovující kategorie. Z následující tabulky můžeme vyčíst, jaké kategorie jsou na trhu a jaké mají jednotlivé parametry.

Kategorie	Druhy kabelů	Frekvence	Rychlost přenosu
1	UTP	Nespecifikováno	Pouze pro přenos hlasu
2	UTP	1 MHz	1 Mb/s
3	UTP, ScTP, STP	16 MHz	4 Mb/s
4	UTP, ScTP, STP	20 MHz	16 Mb/s
5	UTP, ScTP, STP	100 MHz	100 Mb/s
5e	UTP, ScTP, STP	100 MHz	1 Gb/s
6	UTP, ScTP, STP	200 MHz	10 Gb/s
7	UTP, ScTP, STP	600 MHz	

Tabulka 1.1: Kategorie kabelů, zdroj vlastní

### 1.2.2 Optické spoje

Cena pořizovacích nákladů je zde velice vysoká a samostatná instalace s sebou přináší problémy, například maximální ohyb kabelu. Tyto kabely se používají především pro velké vzdálenosti a místa, kde je zapotřebí velmi vysoká odolnost vůči elektromagnetickému rušení. Pro svoji práci bych optické spoje vyloučil a dále se k nim již nevracel.

### **1.2.3 Bezdrátové spoje**

Do bezdrátových spojů patří převážně tyto tři následující přenosy

#### **1.2.3.1 Mikrovlnný přenos**

Jedná se o vnější řešení bezdrátového přenosu dat, který není vhodný pro moji práci a proto se mu nebudu tolik věnovat.

#### **1.2.3.2 Rádiový přenos**

Do rádiového přenosu spadá spousta kategorií a také mnou zvolené technologie Wi-Fi. K tomuto tématu se vrátím v další části práce a budu se jím zabývat do hloubky.

#### **1.2.3.3 Optický přenos**

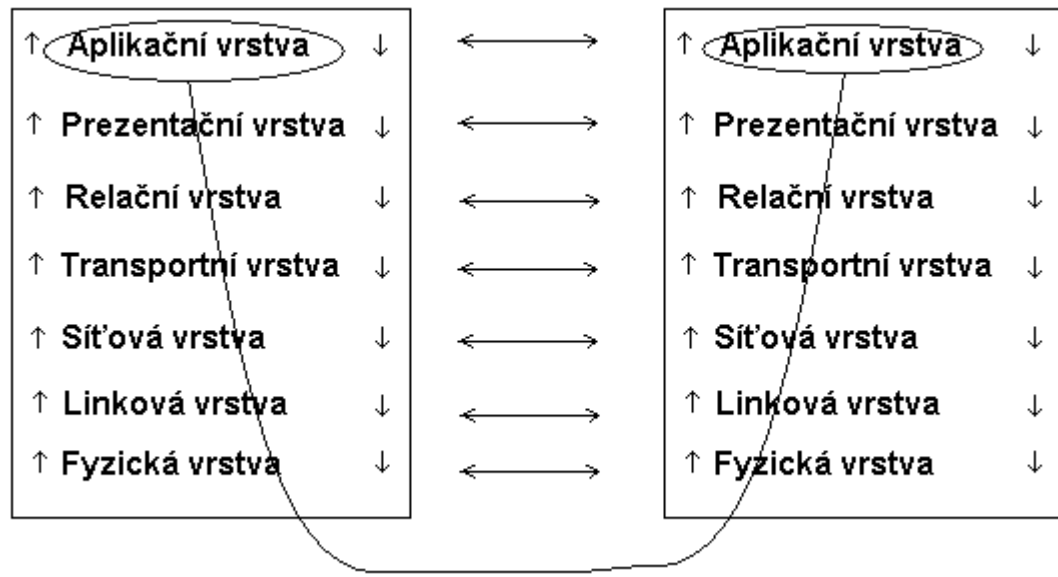
V optických přenosech se používá buď laserový, či infračervený paprsek. Nezbytnou podmínkou pro použití této technologie je bezbariérový přenos paprsků z přijímače na vysílač. Podmínkou je nutnost, aby antény navzájem na sebe viděly. Jelikož tento druh přenosu nebude v mé práci použit, nebudu se jím dále zabývat.

## **1.3 ISO/OSI model**

ISO/OSI je pravděpodobně nejznámějším abstraktním modelem otevřeného systému. Je to určitá norma, která uvádí všeobecné principy sedmivrstvé síťové architektury. Těchto sedm vrstev spolu navzájem spolupracuje vertikálně i horizontálně. Pro lepší představu komunikace nám pomůže obrázek 1.2. Na tomto obrázku je zobrazeno, jak aplikační vrstva na levé straně předá svůj požadavek nižším vrstvám a teprve fyzická vrstva je schopna předat informaci druhému ISO/OSI modelu, kde vše probíhá v opačném pořadí.

Všech sedm vrstev si postupně probereme v jednotlivých kapitolách.

Je důležité vědět, že standard 802.11 definuje jako vlastní pouze dvě nejnižší vrstvy (fyzická a linková). Všechny ostatní nechává standard 802.11 nedotčené. Informace v následujících podkapitolách jsem čerpal převážně z [3], [11] a [15].



**Obrázek 1.2:** Komunikace v ISO/OSI modelu, zdroj vlastní

### 1.3.1 Fyzická vrstva

#### **Ethernet**

Fyzická vrstva nám specifikuje bitový přenos z jednoho zařízení na druhé. Zde hovoříme o samostatném médiu, po kterém je signál přenášen. Tato vrstva si není vědoma obsahu dat. Způsob přenosu může být buď sériový nebo paralelní. Veškeré informace jsou zde kódovány pomocí jedniček a nul. Datové jednotky, které jsou přenášeny fyzickou vrstvou, nazýváme bity.

#### **802.11**

Viz následující kapitoly – 1.7.1 DSSS, 1.7.2 FHSS, 1.7.3 OFDM

### 1.3.2 Linková vrstva

#### **Ethernet**

Linková vrstva provádí rozdělení dat, která přicházejí z vyšší vrstvy do menších celků, tzv. rámců. Tyto rámce jsou předány fyzické vrstvě a následně přenášeny v síti. Při vytváření rámců je možné postupovat dvěma způsoby:

1. Nejmenším stavebním prvkem je jeden znak (znakově orientovaný protokol). Tento způsob je starší a poskytuje méně funkcí. Např. protokol SLIP, který je používán v operačním systému Unix.
2. Nejmenším stavebním prvkem je jeden bit (bitově orientovaný protokol). Tento způsob je moderní a výkonný. Poskytuje jednoduchou ochranu před chybami v přenosu. Je bohatší na podporované funkce. Např. protokol PPP používán pro připojení přes modem.

### **802.11**

Pro práci v bezdrátové síti 802.11 je podvrstva linkové vrstvy nazývána MAC, tedy ovládání přístupu k médiu. Tato podvrstva MAC slouží jako rozhraní mezi fyzickou vrstvou a hostitelským zařízením. Dále vytváří podporu ad-hoc a ifrastrukturálního zapojení sítě. Pro robustnost podvrstvy MAC jsou důležité tyto dvě hlavní vlastnosti. První z nich se nazývá CRC (Cyclic Redundancy Check), tedy cyklický kontrolní součet. Druhá vlastnost se nazývá fragmentace paketů.

Každý z přenášených paketů je opatřen připojeným kontrolním součtem CRC. Díky tomuto kontrolnímu součtu je možné zjistit, zda přenášený paket nebyl během přenosu poškozen, nebo změněn.

Funkce fragmentace paketů rozděluje samostatné pakety na menší kousky a ty přenáší postupně. Na rozdíl oproti kabelovému ethernetu je totiž výrazně vyšší možnost chyby během přenosu paketu a opakovaný přenos celého paketu by síť zbytečně vytěžoval. Pokud je přenášena pouze část tohoto paketu, síť to ušetří mnoho kapacity. Navíc pravděpodobnost poškození přenášeného paketu narůstá s jeho velikostí.

### **1.3.3 Síťová vrstva**

Síťová vrstva si plně uvědomuje topologii sítě. Nemusí tedy řešit přenos informací mezi dvěma body, ale rozhoduje o tom, jakým způsobem budou data putovat v síti. Síťová vrstva stejně jako linková definuje své celky dat pro síťovou vrstvu – pakety. Síťový paket je transformován na linkový rámeček. Obecně existují dva způsoby, jak síťová vrstva posílání paketů řídí. Používá buď virtuální kanál, nebo datagramovou službu.

U Virtuálního kanálu při přenosu vznikne pevné spojení mezi dvěma počítači. Celý proces funguje tak, že vysílací počítač vyšle do sítě první paket a propojovací zařízení určí, kterým směrem se dostane k cíli. Tento první paket zanechá za sebou stopu, po které se následně vydají všechny další pakety. Jakmile se přenos ukončí, je třeba tento virtuální kanál odstranit. Toto tzv. “zametení stop“ provádí poslední paket.

Datagramová služba předává každý paket propojovacímu zařízení samostatně (každý přenášený paket může jít jinou cestou v síti). Výhoda této služby spočívá v tom, že pružně reaguje na změny v síti (poruchy spojení a nebo odstranění uzlu).

### **1.3.4 Transportní vrstva**

Transportní vrstva slouží jako prostředník mezi vyššími a nižšími vrstvami síťového modelu. Jejím úkolem je přebrat od vyšších vrstev data ve formě aplikací a transformovat je na pakety, které jsou pak vkládány do paketů a rámců nižších vrstev. Transportní vrstva poskytuje uživateli představu o naprosto bezchybném síťovém spojení (tzv. podporuje ochranu paketů před poškozením či duplikací).

### **1.3.5 Relační vrstva**

Relační vrstva má dva základní úkoly. První z nich je dialog mezi zařízeními. Řízení dialogu spočívá v určování, které zařízení bude zrovna v daný moment komunikovat. Druhým úkolem je vkládání synchronizačních značek. Toto vkládání nám umožňuje návrat v komunikaci, například při chybě spojení, popřípadě odvolat poslední zvolenou akci.

### **1.3.6 Prezentační vrstva**

Prezentační vrstva mění data, která jí procházejí. Má tři základní modifikace:

- **Překlad dat mezi různými formáty** – např. rozdílné uložení informací v paměti pro procesory Intel a Motorola.

- **Komprimace dat** – příkladem může být bezztrátová komprimace jako je Hoffmanovo komprimování, nebo ztrátová komprimace, jako je MP3 či JPG.
- **Šifrování dat** – máme zde opět dva druhy šifrování. První z nich je symetrické šifrování, které používá pro kódování a dekódování stejný klíč. Druhý z nich je asymetrické kódování, které používá dvojici klíčů. Jeden z nich slouží pro kódování, druhý z nich slouží pro dekódování.

### 1.3.7 Aplikační vrstva

Návrh této vrstvy pochází již z počátku vývoje počítačových sítí. V této době již každá aplikace řeší tuto část síťové komunikace sama pomocí svých prostředků.

## 1.4 Propojovací zařízení

Tyto zařízení slouží pro zapojení více zařízení do sítě, zlepšují její vlastnosti a směřují pakety po síti.

Více o problematice, kterou rozebírají následující podkapitoly se dozvíte v [4], [5].

### 1.4.1 Repeater (opakovač)

Toto zařízení pracuje na úrovni fyzické vrstvy ISO/OSI modelu. Jeho funkcí je zesílení a tvarování signálu. Signál obdržený na jednom portu zopakuje do ostatních portů, přičemž signál přechází, tj. obnoví ostré vzestupné a sestupné hrany.

### 1.4.2 Hub (rozbočovač)

Toto zařízení také pracuje na úrovni fyzické vrstvy ISO/OSI modelu. Dělí se na dvě základní modifikace. První z nich je „pasivní“, která pouze rozesílá signál do všech ostatních připojených zařízení. Druhá se značí jako „aktivní“. Tato modifikace stejně jako „pasivní“ rozesílá signál do všech ostatních připojených zařízení a navíc má v sobě funkci opakovače (zesiluje a tvaruje signál).

### **1.4.3 Switch (přepínač)**

Toto zařízení má dvě možnosti označení. Z pohledu linkové vrstvy ISO/OSI modelu představuje inteligentní variantu mostu, pro síť je transparentní. Z pohledu síťové vrstvy funguje jako rychlý směrovač a v síti lze adresovat. Přepínač je velmi podobný rozbočovači. Na rozdíl od rozbočovače neposílá data na všechny své výstupy, ale jen tam, kam jsou data adresována. Díky tomuto adresování nedochází ke kolizím ve vysílání signálu.

### **1.4.4 Router (směrovač)**

Směrovač pracuje v síťové vrstvě ISO/OSI modelu. Směrovač posílá data po síti tak, aby prošla co nejrychleji. To znamená, že se snaží využívat větve sítě, které jsou méně zatížené. Možné cesty vyhledává na základě routovacích tabulek a snaží se data posílat co nejefektivněji. Odeslaná data zároveň kontroluje, zda jsou v pořádku a zda je znám jejich příjemce. Data, která nejsou v pořádku, zahazuje. Díky tomuto se snižuje celkové zatížení sítě.

### **1.4.5 Brána (gate)**

Brána pracuje na transportní až aplikační vrstvě ISO/OSI modelu a slouží jako tzv. překladatel. Propojuje síť s odlišnými protokoly či s rozdílnou technologií. Brána se může například nacházet mezi sítí Ethernet a sítí Token ring.

### **1.4.6 Most (bridge)**

Technologie most dělí jednu kolizní doménu na více domén. Pracuje na linkové vrstvě ISO/OSI modelu. Pomocí MAC adres rozpoznává, do jaké kolizní domény počítač patří. Stejnou funkci plní i směrovač, ale ten na rozdíl od mostu rozhoduje podle IP adresy.

## 1.5 Přístupové metody

Tyto techniky popisují pravidla, kterými se řídí přístup síťových stanic. V podstatě jde o to, jak zabezpečit, aby do sítě vysílala v jednom okamžiku pouze jedna stanice. Při současném vysílání více stanic dojde k vzájemnému rušení, což znemožní přesun dat.

Informace o následujících technikách lze čerpat z [9] a [3].

### 1.5.1 CSMA/CD – metoda náhodného přístupu (drátový ethernet)

Jedná se o metodu náhodného přístupu. Stanice, která chce vysílat, zkontroluje, zda již nevysílá jiný počítač. Pokud tomu tak je, počká, až bude na síti klid. Když zjistí, že je síť volná, začne vysílat. Může se však stát, že ve stejnou dobu začne vysílat i jiná stanice. Proto vysílací stanice kontroluje, zda signály šířící se sítí odpovídají tomu, co sama vysílá. Pokud tomu tak není, stanice se odmlčí a po náhodné době se pokusí o nové vysílání.

### 1.5.2 CSMA/CA - Vícenásobný přístup s předcházením kolizí (bezdrátový ethernet)

Jedná se o systém předcházení kolizí. U bezdrátových sítí vzniká totiž problém tzv. „skrytého uzlu“. Tento skrytý uzel může omezit komunikaci v síti až o čtyřicet a více procent. Jde o to, že stanice dokáže detekovat, že je volné přenosové médium ve svém okolí, ale nedokáže detekovat, zda přenosové médium je volné i v okolí přijímací stanice.

Používá se zde mechanismus pro předcházení kolizí spolu s kladným potvrzováním. To znamená, že stanice naslouchá a pokud je médium volné, počká určený čas (DIFS) a teprve potom začne vysílat. Příjemce zkontroluje CRC kontrolní součet přijatého paketu a odešle zpět potvrzení ACK. Příjem potvrzujícího paketu znamená pro odesílací stanici, že nedošlo ke kolizi. Pokud stanice paket ACK nedostane, opakuje vysílání.

## 1.6 Typy bezdrátových sítí

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

nazýváme Basic Service Area (BSA). Pokud se stanice nachází v rámci BSA, můžeme komunikovat s dalšími členy BSS. Rozpoznáváme dva hlavní typy sítí podle toho, jak komunikace mezi členy BSS probíhá.“ [3, 15 s]

Informace o těchto hlavních typech sítí byli čerpány z [3].

### **1.6.1 Ad-hoc sítě**

V tomto druhu sítě stanice spolu navzájem komunikují přímo a nepotřebují pro tuto komunikaci žádného prostředníka. Výhodou sítí ad-hoc je jednoduchost v tom smyslu, že není zapotřebí žádný přístupový bod. Tento druh sítě je vhodný pro přenos dat na malé vzdálenosti (řádově několik metrů) a pro menší sítě. Využívá se například k náhlé potřebě přenosu dat mezi notebooky. Po tomto přenosu sítí ovšem zaniká. Sítě Ad-hoc nejsou tak populární vzhledem k jejich malému rozsahu a nutnosti specifické konfigurace.

### **1.6.2 Infrastrukturní sítě**

V infrastrukturních sítích komunikace probíhá přes přístupový bod (access point, AP). Tento přístupový bod slouží jako tzv. datová brána (poskytuje rozhraní mezi bezdrátovou a drátovou sítí).

#### **1.6.2.1 Asociace přístupovým bodem**

V infrastrukturní síti musí být stanice asociována pomocí přístupového bodu. Bez přístupového bodu vytvoření sítě není možné. Asociační proces probíhá tak, že stanice požádá přístupový bod o přihlášení do sítě a ten ji následně povolí či odmítne přístup. Pracovní stanice nemůže být zároveň pomocí jedné síťové karty přihlášena do více sítí. Ze strany přístupového bodu toto omezení neplatí a standard neurčuje, kolik pracovních stanic smí být k přístupovému bodu přihlášeno. Většina přístupových bodů může zvládnout zhruba 253 najednou připojených pracovních stanic. Pro moje využití v této práci bude zároveň přistupovat zhruba 20 pracovních stanic.

### **1.6.2.2 Rozšířená oblast služeb (Extended service area)**

Pro vytvoření rozsáhlé sítě je zapotřebí propojit BSS (AP s připojenými stanicemi) do takzvaných „rozšířených souborů služeb“ (ESS). ESS vytvoříme tím, že propojíme jednotlivé BSS páteřní sítí. Všechny přístupové body musí být nakonfigurovány jako části jedné ESS. Po tomto nastavení veškeré stanice uvnitř ESS mohou mezi sebou komunikovat, přestože jsou v rozdílných BSS. Zároveň se mohou pohybovat i mezi jednotlivými BSS. Nejdůležitějším faktorem při vytváření ESS je nutnost zapojení páteřní sítě do jedné doménové vrstvy. To znamená, že přístupové body musí být zapojeny do stejného přepínače, rozbočovače či směrovače.

## **1.7 Přenosové techniky standardů 802.11**

### **1.7.1 DSSS**

DSSS (Direct Sequence Spread Spectrum) pracuje tak, že každý bit který je přenášen, je před každým přenosem nahrazen určitou skupinou bitů (chipů). Pro jejich vytvoření se u Wi-Fi používá Bakerovo kódování. Jedná se o náhodné sekvence, což představuje výhodu v tom, že je možné, aby v jednom místě koexistovalo více nezávislých sítí (jelikož má každá jiný sekvenční kód). Teprve po vytvoření této sekvence je můžeme začít vysílat a tedy modulovat na nosný signál. Díky této technologii je zpráva šířena v daleko širším spektru a ne všechny chipy jsou pro správnou demodulaci signálu potřebné. Kdybychom neznali způsob, jak je každý bit zakódován, náhodnému posluchači by se přenos jevil jako směs nesouvislých a rušivých signálů (náhodný šum). Díky tomu není možné tento signál demodulovat. [21]

### **1.7.2 FHSS**

FHSS (Frequency Hopping Spread Spectrum) funguje na principu přeskokování frekvencí. Tato technologie pracuje s pásmem 2,4 GHz s maximální rychlostí přenosu 2 Mb za vteřinu. Toto pásmo se rozdělí do nezávislých kanálů o šířce 1 MHz. Čas strávený na každé frekvenci mezi samostatným přeskočením na další je maximálně 400 ms. [10]

### **1.7.3 OFDM**

OFDM (Orthogonal Frequency Division Multiplexing) je druh přenosové techniky pracující s takzvaně rozprostřeným spektrem. Přenosové pásmo je rozděleno na velké množství úzkých kanálů. Signál je zde vysílán ve více na sobě nezávislých frekvencích. Takto přenesený signál zvyšuje odolnost vůči vzájemnému ovlivňování. Konečná rychlost přenosu je součet všech kanálů, a to až 54 Mb/s. [3]

### **1.7.4 MIMO**

MIMO (Multiple Input, Multiple Output) je takzvaná technologie chytrých antén. Tuto technologii využívá nový standard 802.11n. Funguje na principu vysílání několika datových signálů naráz různými telekomunikačními cestami, avšak v rámci jednoho přenosového kanálu. Tato technologie může využívat až 16 antén pro venkovní provoz a až 4 antény pro provoz uvnitř budov. Technologie MIMO zvyšuje přenosovou vzdálenost a také přenosovou rychlost. Teoretická rychlost s použitím MIMO u standardu 802.11n dosahuje 300 Mb/s, reálná rychlost se pohybuje kolem 130 Mb/s. [21]

## **1.8 Rodina standardů IEEE 802.11**

Roku 1990 začala organizace IEEE vytvářet normu, která by umožnila vytvoření bezdrátové sítě z komponentů od různých společností. Dříve totiž bylo možné vytvářet bezdrátové sítě pouze s komponenty od jednoho výrobce. Po sedmi letech vývoje, tedy roku 1997 byl vytvořen první standard IEEE 802.11. Jednotlivé standardy rozeberu hlouběji v následujících kapitolách. [7]

Informace o následných podkapitolách jsem čerpal z [14] a [22].

### **1.8.1 IEEE 802.11**

Tento standard využívá bezlicenční pásmo od 2,4 do 2,4835 GHz. Maximální přenosová rychlost u tohoto standardu je pouze 2 Mb/s. Bohužel tato pomalá rychlost

a nízké zabezpečení jsou nedostačující a bylo zapotřebí nových doplňků, které tento standard upravují.

### **1.8.2 IEEE 802.11a**

Standard IEEE 802.11a byl schválen roku 1999. Nyní pracuje v pásmu 5 GHz s výrazně vyšší přenosovou rychlostí, a to až 54 Mb/s. Byla zde poprvé použita technologie OFDM. Výhodou oproti původnímu standardu není pouze vyšší rychlost, ale také použití vyššího kmitočtového pásma, které je méně vytížené a taky dovoluje využití více kanálů bez vzájemného rušení.

### **1.8.3 IEEE 802.11b**

Standard IEEE 802.11b vznikl zároveň s IEEE 802.11a roku 1999. Pracuje v pásmu 2,4 GHz, a to s maximální rychlostí 11 Mb/s. Využívá nový způsob kódování, tzv. doplňkové kódové klíčování s použitím DSSS. Nastanou-li špatné podmínky přenosu (např. silné zarušení frekvenčního pásma), používá principu dynamické změny přenosové rychlosti. Při slábnutí signálu může přenosová rychlost klesnout na 5,5 Mb/s nebo dokonce 1-2 Mb/s. Jakmile je signál opět dostatečně silný, rychlost se zvýší na její původní maximum 11 Mb/s.

### **1.8.4 IEEE 802.11g**

Tento standard byl schválen v roce 2003. Stejně jako standard IEEE 802.11b využívá pásmo 2,4 GHz. Maximální rychlost přenosu je stejná jako u standardu IEEE 802.11a. Pro dosažení této rychlosti používá technologii OFDM, a navíc používá DSSS pro zpětnou kompatibilitu s IEEE 802.11b. Pro modulaci se používá podle hodnoty odstupu signálu od šumu QPSK (Quadrature Phase Shift Keying), BPSK (Binary Phased Shift Keying), 16-QAM (Quadrature Amplitude Modulation) nebo 64-QAM. Podporované rychlosti v závislosti na jejich modulaci jsou následující: 54 Mb/s (64-QAM), 48, 36 a 24 Mb/s (16-QAM), 18 a 12 Mb/s (QPSK), 9 a 6 Mb/s (BPSK). Další rychlosti jsou stejné

jako u IEEE 802.11b: 11 Mb/s (CCK), 5,5Mbit/s (CCK), 2 Mb/s (DQPSK) a 1 Mb/s (DBPSK). Tento standard je v současnosti nejpoužívanější a jeho nástupcem by měl být standard IEEE 802.11n.

### **1.8.5 IEEE 802.11n**

Standard IEEE 802.11n se začal vyvíjet v roce 2003, jelikož bylo zřejmé, že rychlost předcházejícího standardu IEEE 802.11g bude již brzy nedostačující. S neustálým vývojem byli vytvářeny jednotlivé „mezispecifikace“. V září roku 2009 byl standard IEEE 802.11n konečně schválen. Teoretická rychlost dosahuje až 450 Mb/s, reálná rychlost je zatím 200 Mb/s. Dosažení této rychlosti je možné díky již zmíněné technologii MIMO. Velikou výhodou tohoto standardu je zpětná kompatibilita se standardy IEEE 802.11b/g. Díky této zpětné kompatibilitě můžeme bez problémů postupně přecházet na zařízení s podporou IEEE 802.11n a nemusíme se obávat toho, že nám síť přestane fungovat. Bohužel použití technologie MIMO má i své nevýhody. Hlavní nevýhodou je to, že tato technologie používá více kanálů zároveň a proto v bezlicenčním pásmu, které je v nynější době velice vytížené, bývá přenosová rychlost výrazně nižší, než-li v ideálních podmínkách.

## **1.9 Bezpečnostní mechanismy Wi-Fi sítě**

Pro bezdrátové sítě je nezbytné použití určitého zabezpečení, jelikož každý uživatel, který má zařízení s bezdrátovou kartou, se může připojit do této bezdrátové sítě, na rozdíl od metalických sítí, kde bylo zapotřebí fyzické zásuvky nebo kabelu. Nyní se podíváme na základní zabezpečení, které nám bezdrátové sítě nabízejí.

### **1.9.1 SSID**

SSID (Service Set Identifier) je unikátní identifikátor každé bezdrátové počítačové sítě. Toto základní zabezpečení spočívá v tom, že přístupové zařízení (AP), které v základním nastavení vysílá tento identifikátor (klíč , dlouhý až 32 znaků), jej přestane

vysílat. Uživatel, který by se chtěl do této sítě připojit, jej musí znát. Toto skrytí identity neposkytuje žádnou ochranu dat. Doporučuje se pouze pro doplnění zabezpečení. [16]

### **1.9.2 Filtrování MAC adres**

MAC adresa (Media Access Control) je unikátní identifikátor síťového zařízení, který používá různé protokoly druhé linkové vrstvy ISO/OSI modelu. Tento identifikátor se skládá ze 48 bitů. Mívá podobu šestice dvojciferných hexadecimálních čísel, které jsou odděleny pomlčkami nebo dvojtečkami (např. 02-54-48-76-02-FG). Další formát, s jakým se můžeme setkat, je trojice čtyř hexadecimálních čísel oddělených tečkou (např. 0123.4567.89AB).

MAC adresy jsou přidělovány výrobcem a jsou vždy celosvětově jedinečné. Princip přidělování MAC adres je rozdělen na dvě poloviny. O první polovinu MAC adresy si musí výrobce požádat centrálního správce adresního prostoru a ta je potom u všech síťových karet jednoho výrobce stejná. Druhá polovina tohoto identifikátoru již záleží pouze na výrobcu. Jedinou podmínkou je, že musí být vždy unikátní. Díky jednoznačnosti MAC adres se můžeme spolehnout na věrohodnou identifikaci síťové karty v počítačové síti. Dále usnadňuje správu lokálních sítí.

V přístupovém bodu (AP), je správce sítě schopen aktivovat filtr MAC adres. V tomto filtru se nachází seznam povolených adres, které musí správce zadávat manuálně (což je časově náročné a neefektivní). Pokud uživatel, který se snaží připojit na bezdrátovou síť s aktivním filtrem MAC adres není v seznamu povolených adres, je mu přístup zamítnut. [12]

### **1.9.3 WEP**

WEP (Wired Equivalent Privacy) nám zajišťuje šifrování veškerých rámců v bezdrátové komunikaci. Vše probíhá na úrovni třetí síťové vrstvy ISO/OSI modelu. WEP používá tajné klíče pro šifrování. Přístupový bod (AP) a komunikující stanice musejí tento tajný klíč znát. Jedná se o symetrický princip, kde se pro šifrování a dešifrování používá stejný algoritmus, i totožný statický klíč. K tomuto šifrování se používá algoritmus RC4.

Algoritmus RC4 je nejpoužívanější proudová šifra v softwarových aplikacích. Byl navržen Ronem Rivestem v roce 1987. Do roku 1994 byl držen jako obchodní tajemství. Vstupem RC4 je klíč o volitelné délce, teoreticky až 256 bajtů. Klíč inicializuje konečný automat, který pak generuje posloupnost bajtů hesla  $h(0), h(1), \dots$ . Při zašifrování se heslo „xoruje“ na otevřený text a při odšifrování na šifrovaný text, tedy:  $št(i) = ot(i) \text{ xor } h(i), i = 0, 1, \dots$

Bohužel WEP nijak neřeší distribuci klíče. Jak odesílatel, tak i příjemce musejí mít stejný klíč používaný k šifrování a dešifrování vzájemné komunikace. Z tohoto důvodu je nutné průběžně klíče obměňovat, aby nebyla narušena bezpečnost sítě. Tato obměna klíče musí být provedena ručně, což je časově náročné. Další nevýhodou této změny klíče je nebezpečí, že případný útočník může tento klíč získat při předání.

WEP nám poskytuje dva druhy klíčů. Jedná se buď o 64 bitový a nebo 128 bitový klíč. Čím je klíč delší, tím nám poskytuje relativně vyšší úroveň zabezpečení. Ve skutečnosti jsou uživatelské klíče dlouhé pouze 40 bitů a 104 bitů. Zbýlých 24 bitů využívá proměnná s názvem „Inicializační Vektor“ (IV).

Jakmile začne vysílání paketů, jsou šifrovány pomocí kombinace IV a tajného klíče. IV je teoreticky pro každý paket jiný, zatímco tajný klíč je staticky stanoven. Výsledné datové pakety vypadají jako náhodná data, a proto pro uživatele, kteří neznají klíč, jsou nečitelná. Příjemací stanice obrací proces šifrování, aby získala zprávu jako prostý text. Bohužel hodnoty IV mohou být znovu použity a jeho délka je příliš krátká. 24 bitové klíče umožňují pouze 16,7 milionů možností. I když se to může zdát hodně, ve vytížené síti toto číslo může být dosaženo během několika hodin. Opětovné použití je pak nevyhnutelné a šifra je napadnutelná řadou útoků. [20], [18], [23]

#### **1.9.4 WPA**

WPA (Wi-Fi Protected Access) vznikl v roce 2001 a vychází z koncepce WEP. Byl navrhnout pro odstranění největších nedostatků původního WEP tj. statické klíče. WPA standardně používá 128bitový dynamický klíč, který se mění každých 10 000 paketů a 48bitový inicializační vektor (IV). K hlavním zlepšením patří požití protokolu TKIP

(Temporal Key Integrity Protocol), který dynamicky mění již zmíněné klíče. O další vylepšení vůči šifrování WEP se stará MIC (Message Integrity Check), které slouží jako ochrana proti falešným přístupovým bodům. MIC je používán současně s CRC32 (detekční a opravný kód) a tím řeší jeho nedostatky, díky kterým bylo možné změnit zprávu při zachování stejného kontrolního součtu.

### **1.9.5 WPA2**

Roku 2004 byl schválen zcela nový dodatek 802.11i, který bývá označován jako WPA2 a zcela nahrazuje původní WEP. Zásadním rozdílem mezi WPA a WPA2 je , že WPA2 přichází s blokovou šifrou AES (Advanced Encryption Standard), na rozdíl od původní RC4. Bloková šifra AES využívá symetrického klíče o délce 128, 192 nebo 256 bitů. Tato metoda šifruje data postupně v blocích s pevnou délkou 128 bitů. Šifra se vyznačuje vysokou rychlostí šifrování.

Další změny, která WPA2 přináší jsou například oddělení autentizace a kontrola integrity zprávy. Na základě tohoto je schopna poskytnout stabilní a flexibilní bezpečnostní architekturu, která se dá použít jak pro malou domácí síť, tak pro velkou firemní síť. Tato nová architektura bezdrátových sítí se jmenuje RSN (Robust Security Network). RSN využívá autentizaci 802.1x (vysvětleno níže), silnou distribuci klíčů a také nové mechanismy k zajištění integrity a soukromí. Přestože architektura RSN je složitější, nabízí bezpečná a škálovatelná řešení pro bezdrátovou komunikaci. Ve většině případech RSN akceptuje pouze zařízení s podporou RSN, nicméně IEEE 802.11i definuje také architekturu TSN (Transitional Security Network), u které lze zahrnout jak systémy RSN, tak systémy WEP. [6]

### **1.9.6 IEEE 802.1X**

Pro pochopení, co přináší specifikace IEEE 802.1x musíme nejprve porozumět těmto technologiím.

**PPP (Point to Point Protocol)** – je znám převážně jako protokol pro přístup k internetu za použití telefonních linek, nyní je používán některými poskytovateli DSL a

kabelového připojení k autentizaci. Dříve, než dojde k čemukoliv na 3. vrstvě modelu OSI (např. IP), zajistí protokol PPP ověření uživatele na vrstvě druhé. Obecně se požaduje jméno a heslo. Ověření protokolem PPP je použito vždy pro identifikaci uživatele na druhém konci spojení předtím, než je mu přístup umožněn. Ověřením na 2. vrstvě je uživatel nezávislý na protokolech vyšší vrstvy a může dojít k rozhodnutí, jak naložit s protokolem 3. vrstvy OSI.

Původně zde byly implementovány dvě metody – PAP (Password Authentication Protocol) a CHAP (Challenge Authentication Protocol), ale zde se ukázala jedna slabina, kterou bylo potřeba posílit. Jedná se totiž o poměrně slabé ověřovací metody.

**EAP (Extensible Authentication Protocol)** – je nový autentizační protokol, který je implementován do protokolu PPP a poskytuje obecný rámec pro několik jiných autentizačních metod. Tento protokol byl původně definován v RFC 2284 a následně revidován v RFC 2284bis. EAP byl ze začátku určen pouze pro protokol PPP. Zajišťuje tzv. transportní mechanismus pro všechny druhy ověřovacích metod, nicméně není jeho nedílnou součástí. Na serveru vzdáleného přístupu (RAS) je vytvořen tunel mezi klientem a skutečným ověřovacím serverem. EAP je alternativou k proprietárním ověřovacím systémům a umožňuje jim snadnou práci s hesly, tokeny i PKI certifikáty. Nezajišťuje ověřování jako takové, ale otevřený transportní mechanismus pro další ověřovací systémy.

V 802.1x aktuální server, převážně RADIUS (Remote Authentication Dial In User Service), provádí autentizaci. Tento server, např. AP nemusí být nijak složitý. Všechny výpočty provádí žadatel a autentizační server. Po úspěšné autentizaci jsou provedeny všechny ostatní služby. Výhodou je, že tyto servery mohou být malé, s malým výpočetním výkonem a nízkou pamětí. 802.1x se používá obecně pro všechny typy LAN. Zásadně spočívá v autentizaci uživatelů, šifrování a bezpečném předávání klíčů. U bezdrátových sítí se ověřování provádí na úrovni portů přístupového bodu. Ověření uživatele spočívá v nalezení jeho záznamu na RADIUS serveru. Následná komunikace probíhá tak, že přístupový bod na základě nalezení přítomnosti klienta odešle výzvu k identifikaci. Klient odešle zprávu, která obsahuje identifikační údaje o klientovi, přístupový bod zprávu přijme a pošle ji RADIUS serveru. Po prohledání celé databáze vyšle RADIUS server

přístupovému bodu zprávu o tom, zda klienta přijmout či odmítnout a přístupový bod ji pošle ještě ke klientovi. Jestliže klient byl přijat do sítě, je pro něj otevřen příslušný port.

Při další komunikaci využívá norma 802.1x k šifrování dynamické klíče, které jsou pouze pro daného klienta, a ty po určitém čase mění. [19], [17]

## **1.10 Možné útoky na bezdrátové sítě**

V kapitole bezpečnostní mechanismy Wi-fi sítě byly zmíněny nejpoužívanější bezpečnostní prvky. I přesto, že je bezdrátová síť zabezpečena, nesmíme opomenout možné útoky, které by mohly být vůči ní vedeny. V následujících podkapitolách některé z těchto útoků budou zmíněny.

### **1.10.1 Zjištění SSID**

Zamezení vysílání SSID nám neposkytuje téměř žádnou ochranu. V současné době existuje spousta volně dostupných programů, které dokáží SSID odhalit, přestože bylo jeho vysílání zamezeno na přístupovém bodu.

SSID může být odhaleno buď pasivním, či aktivním útokem. Při pasivním napadení útočník stále sleduje provoz v síti a vyčkává, až se nově příchozí stanice bude snažit na tuto síť připojit. Jakmile k tomu dojde, útočník SSID okamžitě zjistí. V rámci aktivního napadení útočník vyšle některé z připojených stanic odpojovací paket, díky kterému se stanice odpojí a je donucena k opětovnému připojení. Při tomto opětovném připojení útočník odposlechne SSID napadené sítě. [16]

### **1.10.2 Změna MAC adres**

Potencionální útočník je schopen MAC adresu odposlechnout od jiné počítačové stanice, která s přístupovým bodem komunikuje. Jakmile útočník získá MAC adresu, která již je povolena na přístupovém bodu, je pro něj velice jednoduché za použití určitého

nástroje (např. SMAC<sup>1</sup>) tuto adresu nastavit jako vlastní. Po tomto přenastavení na povolenou MAC adresu se útočník může v síti volně pohybovat. [8]

### 1.10.3 Man in the Middle

Útok typu Man in the Middle (tzv. „muž v prostředku“) je považován za jeden z nejnebezpečnějších. Probíhá tak, že potenciální útočník po určitou dobu odposlouchává bezdrátovou komunikaci mezi počítačovou stanicí a přístupovým bodem. Po určitém čase získá a prolomí ukryté SSID přístupového bodu a MAC adresu počítačové stanice. Jakmile útočník získá dostatečné množství informací, pošle odpojovací signál a vytvoří falešný přístupový bod, který se pro počítačovou stanicí chová jako původní přístupový bod, na který byla připojena. Tento útok probíhá tak, aniž by si toho stanice či přístupový bod byly vědomy. Ze strany přístupového bodu se naopak chová jako pracovní stanice a vytváří tak virtuální most (muž v prostředku) v této komunikaci. Data, která přes tento „most“ procházejí, útočník zaznamenává a je díky nim schopen se dostat k citlivým informacím včetně přístupových hesel a certifikátů. [13]

---

<sup>1</sup> SMAC official website [online]. 2009 [cit. 2010-22-04]  
Dostupný z WWW: <<http://www.klcconsulting.net/smac/>>

## 2 ANALÝZA PROBLÉMU

### 2.1 Charakteristika organizace

#### 2.1.1 Základní údaje

<b>Název organizace:</b>	Střední odborná škola Podyjí, s.r.o. (zkratka SOŠ Podyjí s.r.o.)
<b>Kontaktní adresa:</b>	Jarošova 14, 669 02 Znojmo
<b>Datum zřízení:</b>	1. září 1994
<b>Právní forma:</b>	společnost s ručením omezeným (s.r.o.)
<b>Zřizovatel</b>	soukromý
<b>IČ</b>	255 19 395
<b>IZO</b>	108 037 576

#### 2.1.2 Historie

Po událostech v listopadu v roce 1989 nastaly v republice veliké změny, ve kterých nebyly zahrnuty pouze politické změny, ale také změny lidské činnosti. Díky sametové revoluci, která umožnila všem občanům rozvinout jejich schopnosti k realizaci jejich snů, vznikla ve Znojmě jedna z prvních soukromých průmyslových škol stavebních.

Na základě vyhlášky MŠMT ČR č. 353/91 sbírky o soukromých školách byla oficiálně zařazena do sbírky středních škol k datu 1. 9. 1994 jako „ Střední průmyslová škola stavební“ se studijním oborem 36-32-6. Tentýž rok byla jmenována ředitelkou školy **PhDr. Jarmila Ladmanová, CSc.** Pedagogický sbor se skládal ze dvou stálých pracovníků a čtyř externistů. Provoz a výuka na této škole byly hrazeny jak dotacemi MŠMT, tak i příspěvky od rodičů. V roce 1997 po uvolnění prostor bývalé základní školy byly vystavěny nové učebny, laboratoř, počítačová učebna, rýsovný a posilovna. Postupem let v školním roce 1996/1997 škola získala od MŠMT ČR oprávnění k výuce oboru 63-69-6 Veřejnosprávní činnost 6843M. Ve školním roce 2002/2003 byl otevřen nový obor **Správce informačních systémů 26-47-M/004.** [1]

## 2.2 Analýza budovy

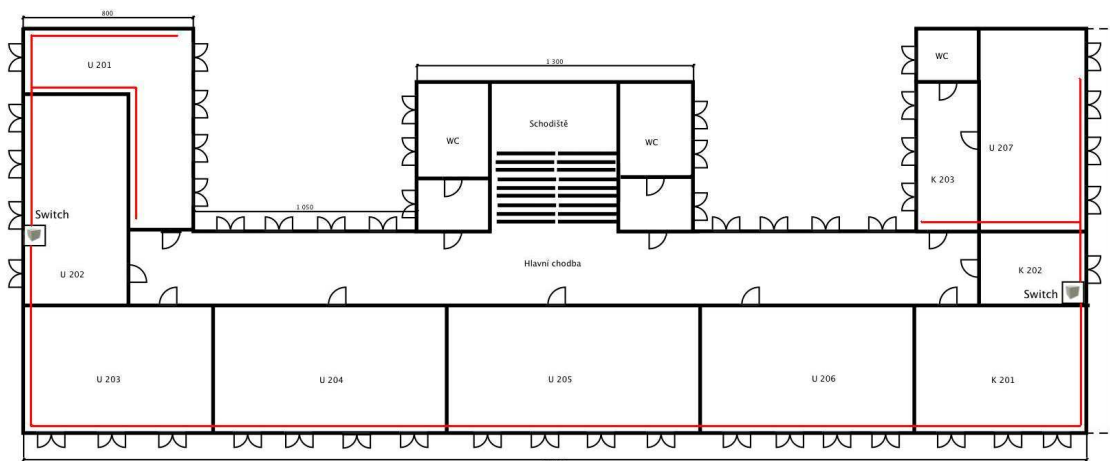
Na obrázku 2.1 můžeme vidět letecký pohled na areál školy SOŠ Podyjí s.r.o., která se nachází ve druhém a třetím patře této budovy. Následně se podíváme na jednotlivá patra a jejich místnosti.



Obrázek 2.1: Budova SOŠ Podyjí s.r.o., zdroj: <http://maps.google.com>

### 2.2.1 První patro budovy školy

V tomto prvním patře (viz. obrázek 2.2) se nacházejí pouze dva aktivní prvky. Jedná se o 20ti portové přepínače L1 od firmy Edimax. Z důvodu, že hlavní server a router se nacházejí až v druhém patře, jsou do tohoto patra vedeny veškeré datové kabely samostatně. Ve třídách U201 a U202 jsou kabely rozvedeny z lokálního přepínače, který je napojen na hlavní router. V kabinetu K201 a třídě U207 jsou kabely také rozvedeny z lokálního přepínače, který je také napojen na hlavní router. Ostatní kabely jsou do tříd vedeny přímo z hlavního patch panelu. Veškerá datová kabeláž je UTP kategorie 6.



**Obrázek 2.2:** Budova – první patro, zdroj: vlastní

V tabulce 2.1 je zaznamenán soupis zásuvek RJ45 pro jednotlivé třídy prvního patra.

Název místnosti	Počet zásuvek 2xRJ45
U201	4
U202	7 (místnost obsahuje aktivní prvek s 20ti porty RJ45)
U203	1
U204	1
U205	1
U206	1
U207	2
K201	4
K202	1 (místnost obsahuje aktivní prvek s 20ti porty RJ45)
K203	1

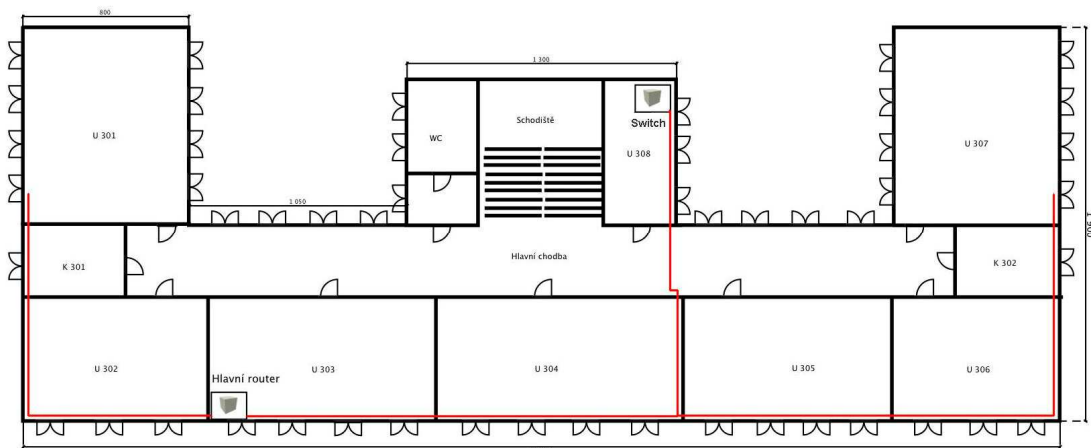
**Tabulka 2.1:** první patro – počty zásuvek RJ-45, zdroj: vlastní

### 2.2.2 Druhé patro budovy školy

Na obrázku 2.3 je patrné, kde se nachází hlavní router. Jedná se o rack skříň, která obsahuje tři přepínače typu L1, dva servery typu W2003, jeden linuxový server Fedora a tři patch panely, z kterých jsou vyvedeny kabely UTP kategorie 6 do všech místností. Nachází se zde také server, na kterém bude spuštěn RADIUS<sup>2</sup> server s veškerou databází a správou uživatelů. Pomocí patch kabelů jsou propojeny veškeré aktivní prvky s patch panely.

<sup>2</sup> The FREE radius project [online]. 2009 [cit. 2010-1-05]  
Dostupný z WWW <<http://freeradius.org/>>

Všechny kabely jsou vedeny v plastových lištách, které jsou na obrázku vyobrazeny jako červené čáry. Ve všech místnostech (mimo toalet) jsou instalovány zásuvky typu 2 x RJ45.



**Obrázek 2.3:** Budova – druhé patro, zdroj: vlastní

V následující tabulce 2.2 nalezneme počty zásuvek RJ45 v jednotlivých třídách druhého patra..

Název místnosti	Počet zásuvek 2xRJ45
U301	1
U302	11
U303	11 (místnost obsahuje aktivní prvky s 70ti porty RJ45)
U304	1
U305	1
U306	1
U307	1
U308	6 (místnost obsahuje aktivní prvek s 12ti porty RJ45)
K301	1
K302	1

**Tabulka 2.2:** druhé patro – počty zásuvek RJ-45, zdroj: vlastní

## 2.3 Analýza rychlosti připojení k internetu

Společnost SkyNet a.s. poskytuje této škole internetové připojení o rychlosti 4 Mb/s download a 4 Mb/s upload. Bude-li tento projekt schválen a realizován, doporučil bych zdvojnásobit tuto rychlost připojení.

## 2.4 Analýza požadavků potenciálních uživatelů

Pro analýzu potenciálních uživatelů jsem se rozhodl vytvořit internetový dotazník na serveru <<http://www.vyplnto.cz>>, který jsem předložil studentům této školy. V následující tabulce můžete vidět výsledky tohoto průzkumu. Na tento dotazník odpovědělo třicet respondentů.

Dotaz:	Odpověď a)	Odpověď b)	Odpověď c)	Odpověď d)
Jste vlastníkem zařízení s podporou Wi-Fi?	Ano (20)	Ne (10)		
Jste vlastníkem notebooku?	Ano (19)	Ne (1)		
Hodláte si zařízení s podporou Wi-Fi pořídit?	Ano (9)	Ne (1)		
Přivítal/a byste Wi-Fi síť v prostorách školy?	Ano (29)	Ne (0)		
Za jakým účelem byste tuto bezdrátovou síť využíval/a?	Vyhledávání podkladů pro účely studia (29)	K využívání sociálních sítí (19)	K hraní her (17)	Za účelem stahování hudby, filmů a programů (12)
Jaká je podle Vás dostačující přenosová rychlost bezdrátové sítě ve školní síti?	< 512 b	512 b – 1 Mb (10)	1 Mb – 4 Mb (19)	> 4 Mb
Jaký je podle Vás dostatečný datový limit přenosu za týden? (jedná li se o školní bezdrátovou síť)	< 50 MB	50 MB – 120 MB (8)	120MB - 200MB (21)	>200 MB

Přivítal/a byste osobní prostor ve školní síti?	Ano (21)	Možná (7)	Ne (1)	
Jste muž nebo žena?	Muž (25)	Žena (4)		

**Tabulka 2.3:** Dotazník potenciaálních uživatelů Wi-Fi

Z tohoto průzkumu je patrné, že žáci této školy mají zájem o vytvoření bezdrátové sítě v prostorách školy. Většina respondentů jsou vlastníky zařízení s podporou Wi-Fi a nebo si je hodlá pořídit. Dále si můžeme všimnout, že všichni respondenti, kteří jsou pro vybudování bezdrátové sítě, by ji využívali převážně k vyhledávání materiálů potřebných ke studiu.

### 3 VLASTNÍ NÁVRH ŘEŠENÍ

Současný vývoj informačních technologií nám nyní poskytuje možnosti, které dříve byly velice špatně realizovatelné a nebo finančně náročné. Nynější výkony počítačů nám umožňují pracovat s náročnými programy, která využívají multimediální technologie. Jelikož se jedná o školu, která ve velké míře využívá tyto informační technologie, je skoro nezbytné být stále připojen k internetu. Jedná se například o potřebu stahování nových aktualizací a pluginů do grafických programů. K většině domácích projektů studenti potřebují počítač. Jedná se například o rýsování, vytváření grafických návrhů, programování programů a tak dále. Tyto úkoly studenti většinou vytváří na svých vlastních počítačích a pokud mají notebooky, mohou s nimi pracovat i ve škole. Bohužel v nynější době nemají možnost se nijak připojit k počítačové síti a tato absence internetového připojení je v této době obrovský nedostatek. Některé programy jsou bez internetového připojení doslova nepoužitelné. Dokonce existuje i operační systém<sup>3</sup>, který bez internetového připojení nefunguje.

Mým úkolem je navrhnout kvalitní bezdrátovou síť, která studentům poskytne připojení k internetu a také vytvoří podmínky vhodné pro interaktivní výuku.

Pro vlastní návrh řešení jsem se rozhodl využít aktivní prvky s podporou standardu IEEE 802.11n. Pro tento standard jsem se rozhodl proto, že se jedná o nejnovější a nejrychlejší finančně dostupný standard na trhu. Jelikož je zpětně kompatibilní i se standardy IEEE 802.11b a IEEE 802.11g, nenastane zde problém s připojením i pro majitele starších notebooků a ostatních zařízení.

#### 3.1 Fáze realizace projektu

- výběr a nákup přístupových bodů
- výběr a nákup antén

---

<sup>3</sup> Chrome OS: Nekompletní recenze nehotového systému [online]. 2009 [cit. 2010-22-04]  
Dostupný z WWW <<http://cleb.blog.root.cz/2009/11/29/chrome-os-nekompletni-recenze-nehotoveho-systemu/>>

- rozmístění antén a přístupových bodů
- zapojení přístupových bodů do páteřní sítě
- úpravy elektrické instalace pro napájení přístupových bodů
- nastavení přístupových bodů

### 3.2 Výběr přístupových bodů

Jelikož přístupových bodů jsou na trhu stovky, rozhodování bylo velice náročné. Mé požadavky na toto zařízení byly zaměřeny především na druhy zařízení s podporou standardu IEEE 802.11n. Tímto kritériem se výběr snížil. Dále jsem se zaměřil na zařízení které mají tři externí antény a také disponují funkcí ověření 802.1x (možnost autentizace za pomoci RADIUS serveru). Po dlouhém hledání jsem se rozhodl zvolit produkt firmy ASUS. Jedná se o bezdrátový router RT-N16 (obrázek tohoto zařízení nalezneme v příloze č. 1). Jeho parametry nalezneme v tabulce níže.

Datové rozhraní	Ethernet, Wi-Fi, USB
LAN Porty	WAN x 1, LAN x 4 RJ-45 pro 10/100/1000 Base T, podpora 802.3
Anténa	3 x externí anténa
USB port	USB2.0 x 2
Napájení	AC vstup 100V – 240V (50 -60HT) DC výstup 12V s maximálně 1,25A
Rozměry	216 mm x 161,9 mm x 40,5 mm
Váha	470 g
Operační pásmo	2,4 GHz– 2,5 GHz
Wi-Fi standardy	IEEE 802.11b/g/n
Regulace propustnosti dat (QoS)	Ano
Kontrola přístupů dle MAC (ACL)	Ano
Další síťové služby	WMM, UPnP, NTP klient, DDNS klient
Šifrování	64/128-bit WEP WPA-PSK, WPA2-PSK WPA-Enterprise, WPA2-Enterprise RADIUS s 802.1x

Síťové protokoly	IC IP, Statická IP, PPPoE (MPPE podpora), PPTP, L2TP
Bezpečnostní prvky	Firewall: NAT a SPI (Stateful Packet Inspection)  Protokolování: Dropped packet, security event, Syslog  Filtrování: Porty, IP packety, URL klíčová slova, MAC adresy

**Tabulka 3.1** Specifikace routeru RT-N16, zdroj:

<[http://www.asus.com/product.aspx?P\\_ID=WAA6AQFncrceRBEo&templete=2](http://www.asus.com/product.aspx?P_ID=WAA6AQFncrceRBEo&templete=2)>

Jedná se o velice výkonné zařízení s obrovskou škálou bezpečnostních prvků. Mezi další výhody tohoto zařízení patří podpora USB. Do portu USB následně můžeme zapojit tiskárnu, nebo pevný disk. Takto zapojený pevný disk může sloužit studentům k distribuci studijních a jiných materiálů. Disk bude přístupný také vyučujícím učitelům, kteří zde budou mít možnost vystavit potřebné materiály pro výuku.

Aby byly pokryty všechny učebny dostatečně silným Wi-Fi signálem, bude zapotřebí nakoupit celkem čtyři tato zařízení.

### 3.3 Výběr antén

Jelikož budova, ve které se škola nachází, má velice tlusté zdi a přístupový bod ASUS RT-N16 nemá dostatečně výkonné antény, je zapotřebí přikoupit antény s vyššími dBi. Pro tento projekt jsem zvolil antény od firmy TP-LINK. Jedná se o anténu TL-ANT2408C 8dBi (obrázek tohoto zařízení naleznete v příloze č. 2). Je to všesměrová vnitřní anténa se ziskem 8 dBi a 1,3m dlouhým kabelem s konektorem RP-SMA.

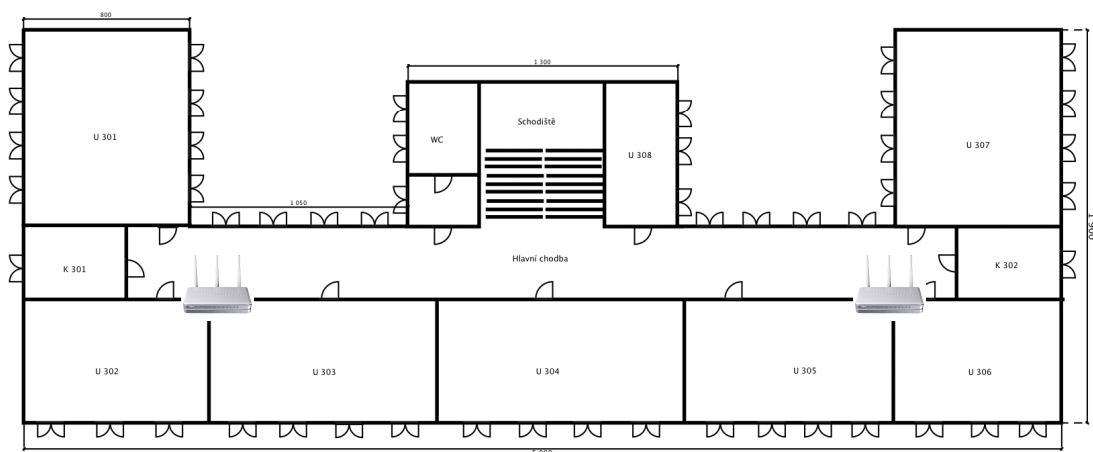
Pro zvýšení efektivity použiji dvě metody, které mi pomohou zvýšit kvalitu a pokrytí celkového signálu.

### 3.4 Rozmístění antén a přístupových bodů

Pro zvýšení efektivity a vhodného využití všech tří antén jsem navrhl vlastní způsob montáže přístupových bodů a jejich antén. Aby bylo zabráněno odcizení, nebo neodbornému zacházení s přístupovými body, budou tato zařízení instalována u stropů v uzamykatelných boxech (obrázek tohoto boxu naleznete v příloze č. 3) na hlavních chodbách. Na každém zařízení budou jednotlivé antény jinak směřovány, v případě potřeby

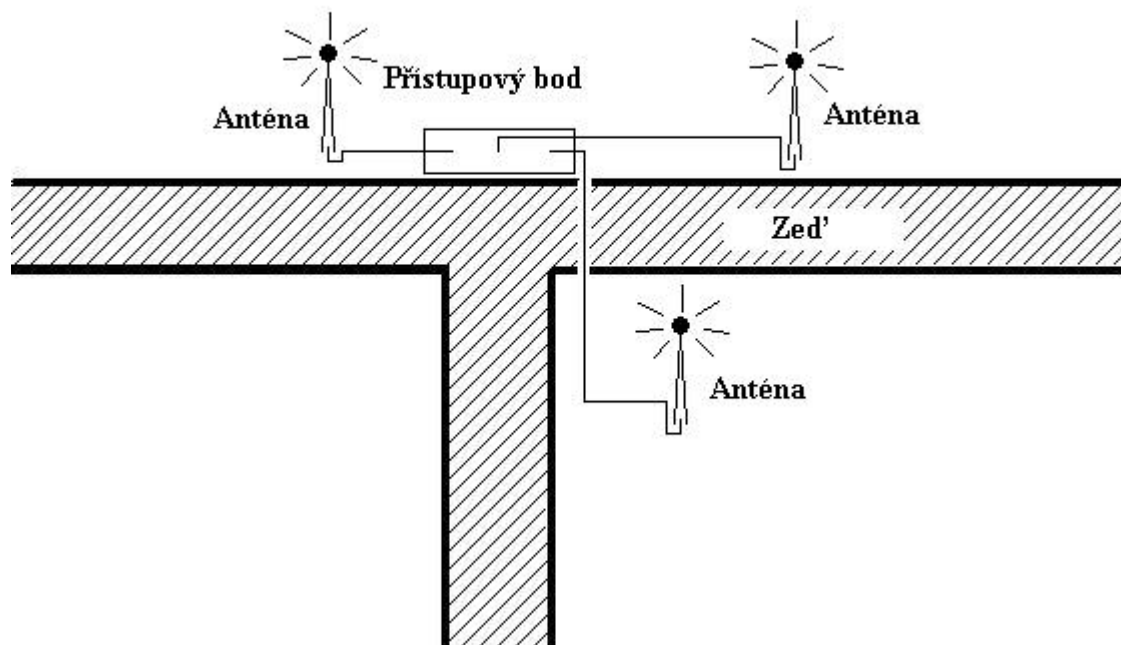
mohou být antény rozšířené o jednoduchý směrovač signálu, viz. „3.4.1 Návrh vylepšení signálu“.

Jelikož chci dosáhnout co nejvyšší efektivity, přístupové body budou umístěny na zdech, které dělí jednotlivé třídy (viz. obrázek 3.3).



**Obrázek 3.3:** Budova - druhé patro s přístupovými body, zdroj: vlastní

Na následujícím obrázku 3.4 „Ukázka řezu zdi“ si můžete všimnout, že dvě antény se budou nacházet přímo na chodbě a třetí z trojice bude nainstalována v přilehlé místnosti.



**Obrázek 3.4:** Ukázka řezu zdi, zdroj: vlastní

### 3.4.1 Návrh vylepšení signálu

Jak již bylo zmíněno, zdi jsou v tomto objektu velmi tlusté, může vzniknout situace, že v některých místech budovy by signál nemusel dosahovat nejvyšší rychlosti. V tomto případě můžeme vytvořit velmi jednoduché směrovače signálu. V následujícím odkazu nalezneme videonávod pro jejich vytvoření.<sup>4</sup>

<sup>4</sup> Jak zdarma zesílit WIFI signál [online]. 2008 [cit. 2010-22-04]  
Dostupný z WWW <<http://www.videoforum.cz/cz/veda-a-technika/detail/veda-a-technika-hobby-videonavody-zabavna-videa-srandovni-videa-zajimave-clanky-jak-zdarma-zesilit-wifi-signal.html>>.

### **3.5 Zapojení přístupových bodů do páteřní sítě**

Do všech přístupových bodů budou přivedeny datové kabely UTP kategorie 6 z co nejbližších volných zásuvek RJ45. Jelikož jsou tyto zásuvky napojeny na patch panel, pomocí patch kabelů, budou dále připojeny do RADIUS serveru. Kabely budou vedeny v plastických lištách, které budou instalovány na omítky zdí.

### **3.6 Úpravy elektrické instalace pro napájení přístupových bodů**

Přístupové body budou umístěny u stropu a je zapotřebí k těmto místům dovést elektrickou energii. Nejprve jsem uvažoval o možnosti napájení po ethernetovém kabelu, ale z důvodu zbytečně vysoké ceny těchto zařízení jsem toto řešení zamítl. Zvolil jsem mnohem levnější variantu. Od nejbližší zásuvky budou nataženy prodlužovací kabely, které budou vedeny v plastových lištách. Tyto kabely povedou k přístupovým bodům a zde budou vytvořeny nové elektrické zásuvky.

### **3.7 Nastavení přístupových bodů**

Všechny čtyři přístupové body budou mít ukryté SSID, které bude následně sděleno všem studentům. Bezdrátový mód bude nastaven na automatický mód (zařízení bude fungovat pro všechny standardy IEEE 802.11b/g/n). Šířka pásma bude nastavena na 40 MHz. Kanál se bude volit automaticky (při vzájemném rušení možno nastavit každý přístupový bod na jiný kanál). Metoda ověření bude zvolena na ověření RADIUS serverem s 802.1x (každý uživatel bude mít vytvořen vlastní přihlašovací účet). Pro zvýšení bezpečnosti doporučuji zapnout filtr MAC adres (každé nově používané zařízení v síti by muselo být přidáno do všech přístupových bodů). Přístupové body budou automaticky vypínat bezdrátový režim v době, kdy bude škola zavřená (časy vypnutí se budou moci editovat podle potřeb školy). Veškeré ostatní nastavení by se upravilo podle představ administrátora školní sítě.

### 3.8 Ekonomické zhodnocení

V následující tabulce 3.2 jsou vypočteny orientační náklady na materiál pro vytvoření bezdrátové sítě na této škole. Tato bezdrátová síť by měla nalákat nové zájemce o studium a ulehčit výuku nynějším studentům. Tuto školu navštěvuje spousta studentů, kteří bydlí ve vesnicích okolí Znojma. V některých případech tito studenti čekají na jejich spoje i několik hodin. Díky této bezdrátové síti, by studenti mohli využít tento volný čas k tvorbě školních projektů, u kterých potřebují podporu internetu.

Na základě této bezdrátové sítě by škola mohla začít uvažovat o zavedení interaktivní výuky a usnadnit studentům jejich studia.

Table

Položka	Počet kusů	Orientační cena s DPH za kus	Orientační celková cena s DPH
Asus RT-N16 N Wi-Fi Router	4	3 293 Kč	13 172 Kč
Anténa TP-LINK TL-ANT2408C	12	280 Kč	3 360 Kč
Box RACK Digitus 6U 10"	4	1 456 Kč	5 824 Kč
Kabel UTP kategorie 6	65 m	6 Kč/m	390 Kč
Koncovka UTP RJ45	8	3 Kč	24 Kč
Plastová lišta na kabel	36 m	62,5 Kč/m	2 250 Kč
Kabel napěťový	20 m	13 Kč/m	260 Kč
Zástrčka 220V samec	4	50 Kč	200 Kč
Zástrčka 220V samice	4	50 Kč	200 Kč
			25 680 Kč

Tabulka 3.2: Náklady na projekt

## ZÁVĚR

Cílem mojí práce bylo vytvořit návrh bezdrátové sítě v prostorách školy. Tato síť by měla sloužit studentům k přístupu na internet. Potřeba internetového připojení je v dnešní době téměř nutností, tato škola však bezdrátovou síť postrádá. I když má své počítačové učebny připojeny k internetu, žáci zde mají přístup pouze ve výuce. Jelikož je internet neomezeným zdrojem informací, spousta žáků pro získávání znalostí dává přednost internetu před literaturou. Jak bylo zjištěno v mém osobním průzkumu na této škole, přes 63% žáků vlastní zařízení s podporou Wi-Fi a ze zbylých 33% žáků si 90% žáků hodlá zařízení s podporou Wi-Fi pořídit. Všichni tito žáci by přivítali pokrytí Wi-Fi na této škole.

Tento projekt na vybudování bezdrátové sítě bude předložen vedení školy a nyní již záleží pouze na vedení, zda tento projekt schválí a bude financovat. Celková částka 25 680 Kč není zas tak vysoký obnos. Jelikož se jedná o nejmodernější technologie, přenosové rychlosti by měly být dostačující nejméně na pět až deset let.

Vytvoření bezdrátové sítě pro studenty by škole zvýšilo prestiž a přilákalo více zájemců o studium na této škole. Na základě infrastruktury této bezdrátové sítě by bylo možné vytvořit tzv. „notebookové“ třídy, kde by výuka probíhala převážně interaktivní formou, jak již na některých konkurenčních školách je realitou. Tato interaktivní forma studia by studentům přinesla větší komfort a mohla by je lépe připravit na budoucí zaměstnání.

# POUŽITÉ ZDROJE

## Knižní zdroje

- [1] PYKALOVÁ, Květoslava *Almanach SOŠ Podyjí s.r.o.* . Vyd. 1. Znojmo: Schneider CZ graphic&design s.r.o., 2005. 48 s.
- [2] TRULOVE, James. *Sítě LAN – hardware, instalace a zapojení*. Vyd. 3. Praha: Grada, 2009. 384 s. ISBN 978-80-247-2098-2
- [3] ZANDL, Patrick. *Bezdrátové sítě WIFI : Praktický průvodce*. Vyd. 1. Brno: Computer Press, 2003. 190 s. ISBN 80-7226-632-2

## Elektronické zdroje

- [4] Aktivní prvky, fyzická a linková vrstva [online]. 2000 [cit. 2010-04-04]. Dostupný z WWW: <<http://www.svetsiti.cz/view.asp?rubrika=Technologie&clanekID=20>>
- [5] Aktivní prvky, síťová vrstva [online]. 2000 [cit. 2010-04-04]. Dostupný z WWW: <<http://www.svetsiti.cz/view.asp?rubrika=Technologie&temaID=&clanekID=21>>
- [6] Bezpečnost Wi-Fi – WEP WPA a WPA2 [online]. 2006 [cit. 2010-04-04]. Dostupný z WWW: <[www.hsc.fr/ressources/articles/hakin9\\_wifi/hakin9\\_wifi\\_CZ.pdf](http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_CZ.pdf)>
- [7] Discover and Learn [online]. 2010 [cit. 2010-04-04]. Dostupný z WWW: <[http://www.wi-fi.org/discover\\_and\\_learn.php](http://www.wi-fi.org/discover_and_learn.php)>
- [8] Enable MAC Address Filtering on Wireless Access Points and Routers [online]. 2004 [cit. 2010-04-04]. Dostupný z WWW: <<http://compnetworking.about.com/cs/wirelessproducts/qt/macaddress.htm>>
- [9] Ethernet po 30 letech (2) - CSMA/CD je když... [online]. 2003 [cit. 2010-04-04]. Dostupný z WWW: <<http://www.svetsiti.cz/view.asp?rubrika=Technologie&clanekID=249>>
- [10] FHSS [online] 2002 [cit. 2010-30-03]. Dostupný z WWW: <<http://www.webopedia.com/TERM/F/FHSS.html>>
- [11] Fyzická a linková vrstva ISO OSI [online]. 2000 [cit. 2010-04-04]. Dostupný z WWW: <<http://www.svetsiti.cz/view.asp?rubrika=Technologie&temaID=&clanekID=14>>

- [12] MAC adresa sítí [online]. 2009 [cit. 2010-01-04]. Dostupný z WWW: <[http://cs.wikipedia.org/wiki/MAC\\_adresa](http://cs.wikipedia.org/wiki/MAC_adresa)>
- [13] Man-In-The-Middle (MITM) Attack Routers [online]. 2007 [cit. 2010-10-04]. Dostupný z WWW: <<http://www.wlanbook.com/wireless-man-in-the-middle-mitm-attack/>>
- [14] Přehled doplňků standardu IEEE 802.11 [online]. 2005 [cit. 2010-30-03]. Dostupný z WWW: <<http://access.feld.cvut.cz/view.php?cisloclanku=2005113002>>
- [15] Síťová a vyšší vrstvy referenčního modelu ISO OSI [online]. 2000 [cit. 2010-04-04]. Dostupný z WWW: <<http://www.svetsiti.cz/view.asp?rubrika=Technologie&temaID=&clanekID=19>>
- [16] SSID [online]. 2010 [cit. 2010-04-04]. Dostupný z WWW: <<http://www.topbits.com/ssid.html>>
- [17] Stavíme bezdrátovou síť - IV [online]. 2004 [cit. 2010-10-04]. Dostupný z WWW: <<http://www.abclinuxu.cz/clanky/site/stavime-bezdratovou-sit-iv>>
- [18] Šifra, která míchá karty [online]. 1999 [cit. 2010-01-04]. Dostupný z WWW: <<http://crypto-world.info/klima/1999/chip-1999-09-42-44.pdf>>
- [19] Technologie pro zlepšení bezpečnosti datových sítí - standard 802.1x (1) [online]. 2004 [cit. 2010-04-04]. Dostupný z WWW: <<http://www.svetsiti.cz/view.asp?rubrika=Technologie&clanekID=261>>
- [20] WEP weaknesses [online]. 2009 [cit. 2010-01-04]. Dostupný z WWW: <<http://www.openextra.co.uk/articles/wep-weaknesses>>
- [21] Wi-Fi 802.11n: průlom nebo propadák? [online]. 2008 [cit. 2010-30-03]. Dostupný z WWW: <[http://www.svethardware.cz/art\\_doc-CF76DF5458DF437CC12574B0004BA010.html?lotus=1&Highlight=0,Wi-Fi,802.11n:,prulom,nebo,propadak](http://www.svethardware.cz/art_doc-CF76DF5458DF437CC12574B0004BA010.html?lotus=1&Highlight=0,Wi-Fi,802.11n:,prulom,nebo,propadak)>
- [22] Wi-Fi certified n Industry [online]. 2009 [ci. 2010-01-04]. Dostupný z WWW: <[http://www.wi-fi.org/register.php?file=wp\\_Wi-Fi\\_CERTIFIED\\_n\\_Industry.pdf](http://www.wi-fi.org/register.php?file=wp_Wi-Fi_CERTIFIED_n_Industry.pdf)>
- [23] Wifi sítě a jejich slabiny [online]. 2005 [cit. 2010-01-04]. Dostupný z WWW: <<http://www.security-portal.cz/clanky/wifi-s%C3%ADt%C4%9B-jejich-slabiny>>
- [24] Základy topologie a komunikace [online]. 2000 [cit. 2010-04-04]. Dostupný z WWW: <<http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&clanekID=21>>

## SEZNAM POUŽITÝCH ZKRATEK

ACK	-	Acknowledge
AES	-	Advanced Encryption Standard
AP	-	Access Point
BPSK	-	Binary Phased Shift Keying
BSA	-	Basic Service Area
BSS	-	Basic Service Set
CRC	-	Cyclic Redundancy Check
CSMA/CA	-	Carrier Sense Multiple Access/with Collision Avoidance
CSMA/CD	-	Carrier Sense Multiple Access/with Collision Detection
DDNS	-	Dynamic DNS
DIFS	-	Distributed Inter Frame Space
DSSS	-	Direct Sequence Spread Spectrum
EAP	-	Extensible Authentication Protocol
ESS	-	Extended Service Set
FHSS	-	Frequency Hopping Spread Spectrum
CHAP	-	Challenge Authentication Protocol
IEEE	-	Institute Of Electrical And Electronics Engineers
ISO	-	International Organization for Standards
IV	-	Initialization Vector
MAC	-	Media Access Control (address)
MIC	-	Message Integrity Check
MIMO	-	Multiple Input and Multiple Output
NEXT	-	Near end Crosstalk
NTP	-	Network Time Protocol
OFDM	-	Orthogonal Frequency Division Multiplexing
OSI	-	Open System Interconnect
PAP	-	Password Authentication Protocol
PPP	-	Point to Point Protocol
QAM	-	Quadrature Amplitude Modulation
QPSK	-	Quadrature Phase Shift Keying
RADIUS	-	Remoute Authentication Dial In User Service
RSN	-	Robust Security Network
ScTP	-	Screened Twisted Pairs
SSID	-	Service Set Identifier
STP	-	Shielded Twisted Pairs
TKIP	-	Temporal Key Integrity Protocol
TSN	-	Transitional Security Network
UPnP	-	Universal Plug and Play
UTP	-	Unshielded Twisted Pairs
WEP	-	Wired Equivalent Privacy
Wi-Fi (WiFi)	-	Wireless Fidelity
WMM	-	Wi-Fi Multimedia
WPA	-	Wi-Fi Protected Access

## SEZNAM OBRÁZKŮ

Obrázek 1.1: Topologie STAR (hvězda), zdroj vlastní .....	13
Obrázek 1.2: Komunikace v ISO/OSI modelu, zdroj vlastní .....	16
Obrázek 2.1: Budova SOŠ Podyjí s.r.o., zdroj: <a href="http://maps.google.com">http://maps.google.com</a> .....	34
Obrázek 2.2: Budova – první patro, zdroj: vlastní.....	35
Obrázek 2.3: Budova – druhé patro, zdroj: vlastní .....	36
Obrázek 3.3: Budova - druhé patro s přístupovými body, zdroj: vlastní.....	42
Obrázek 3.4: Ukázka řezu zdi, zdroj: vlastní.....	43
Obrázek 3.1: ASUS RT-N16 .....	51
Obrázek 3.2: TP-LINK TL-ANT2408C 8dBi .....	51
Obrázek 3.5: RACK Digitus 6U 10" .....	52

## SEZNAM TABULEK

Tabulka 1.1: Kategorie kabelů, zdroj vlastní .....	14
Tabulka 2.2: první patro – počty zásuvek RJ-45, zdroj: vlastní .....	35
Tabulka 2.2: druhé patro – počty zásuvek RJ-45, zdroj: vlastní.....	36
Tabulka 2.3: Dotazník potencionálních uživatelů WiFi .....	38
Tabulka 3.1 Specifikace routeru RT-N16, zdroj: < <a href="http://www.asus.com/product.aspx?P_ID=WAA6AQFncrceRBEo&amp;templete=2">http://www.asus.com/product.aspx?P_ID=WAA6AQFncrceRBEo&amp;templete=2</a> > .....	41
Tabulka 3.2: Náklady na projekt.....	45

## SEZNAM PŘÍLOH

Příloha č. 1: Router ASUS RT-N16.....	51
Příloha č. 2: Anténa TP-LINK TL-ANT2408C 8dBi .....	51
Příloha č. 3: RACK Digitus 6U 10" .....	52

Příloha č. 1: Router ASUS RT-N16



**Obrázek 3.1:** ASUS RT-N16

Příloha č. 2: Anténa TP-LINK TL-ANT2408C 8dBi



**Obrázek 3.2:** TP-LINK TL-ANT2408C 8dBi

Příloha č. 3: RACK Digitus 6U 10"



**Obrázek 3.5:** RACK Digitus 6U 10"