Evropský polytechnický institut, s.r.o.

BAKALÁŘSKÁ PRÁCE

2008 Jakub Syrový DiS.

Evropský polytechnický institut, s.r.o. v Kunovicích

Studijní obor: Elektronické počítače

Návrh bezdrátové počítačové sítě

Autor: Jakub Syrový DiS.

Vedoucí práce: Petr Mareš MBA, John Mikton MA BA

Kunovice, duben 2008

Evropský polytechnický institut, s.r.o.

1. soukromá vysoká škola na Moravě

Osvobození 699, 686 04 Kunovice, tel.: 572 549 018, fax.: 572 548 788
http://www.edukomplex.cz, e-mail: **epi@edukomplex.cz**

Student(ka)
Jakub Syrový
Žichlínek 242
563 01 Lanškroun

Zadání bakalářské práce

Vážený studente, vážená studentko,

jako téma Vaší bakalářské práce ve studiu oboru Elektronické počítače Vám zadávám

Návrh bezdrátové počítačové sítě

Osnova: 1. Analýza hardwarového řešení počítačové sítě
2. Návrh bezdrátové sítě
3. Konfigurace přípojných bodů a měření dostupnosti signálu
4. Testování v rámci mobilní učebny

Bakalářská práce bude zpracována pro: Mezinárodní školu v Praze

Tento dokument je součástí Vaší bakalářské práce.

V Kunovicích 19. března 2008

S pozdravem

Evropský polytechnický institut,
s. r. o.
Osvobození 699
686 04 KUNOVICE

-1-

Oldřich Kratochvíl
Honorary professor, Ing., Dr.h.c.
rektor

Prohlášení

Čestně prohlašuji, že jsem bakalářskou práci na téma Návrh bezdrátové sítě vypracoval samostatně, s využitím pramenů uvedených v použité literatuře a po odborných konzultacích s vedoucím práce Petrem Marešem MBA a panem Johnem Miktonem MA BA.

Kunovice, duben 2008 .....

Podpis

Poděkování

Děkuji vedoucím bakalářské práce Petru Marešovi MBA (in memoriam) a panu Johnu Miktonovi MA BA, za metodické vedení, odborné rady a podnětné připomínky, které mi pomohly při jejím vypracování.

Obsah

1 ÚVOD 8

2 CÍL PRÁCE 9

3 POČÍTAČOVÉ SÍTĚ 10

3.1 TYPY SÍTÍ 10

3.1.1 LAN 10

3.1.2 MAN 11

3.1.3 WAN 11

3.1.4 PAN 12

3.1.5 Sítě typu peer-to-peer 12

3.1.6 Serverové sítě 13

3.2 BEZDRÁTOVÁ SÍŤOVÁ KOMUNIKACE 14

3.2.1 Přenosové techniky 14

3.2.2 Přehled bezdrátové radiové technologie 14

3.2.3 WiFi 19

3.3 PODROBNÝ POPIS IEEE 802.11 20

3.3.1 IEEE 802.11 a model OSI 20

3.3.2 Topologie bezdrátové sítě 22

3.4 HARDWAROVÉ VYBAVENÍ BEZDRÁTOVÝCH SÍTÍ 23

3.4.1 Přístupový bod (Access Point) 23

3.4.2 Softwarový přístupový bod 24

3.4.3 Síťový most 24

3.4.4 Bezdrátový opakovač 24

3.4.5 WiFi síťový adaptér 24

3.4.6 Antény 26

3.4.7 Konektory a kabelová vedení 28

4 SPRÁVA SÍTÍ 29

4.1 SPRÁVA A KONFIGURACE PŘÍSTUPOVÉHO BODU 29

4.1.1 Možnosti konfigurace přístupových bodů 29

4.1.2 Přístup na internet 29

4.1.3 DHCP server 29

4.1.4 Veřejné a privátní IP adresy 30

4.1.5 Firewall 30

4.1.6 DMZ – demilitarizovaná zóna 31

4.1.7 Přesměrování portů 31

4.1.8 Filtrování 31

4.1.9 VPN (Virtual Private Network) 31

5 BEZPEČNOST SÍTÍ 32
5.1 ŠIFROVÁNÍ 32
5.1.1 WEP (Wired Equivalent Privacy) 32
5.2 AUTENTIZACE 33
5.2.1 Open-system autentizace 34
5.2.2 Shared-key autentizace 34
5.2.3 Filtrování adres 34
5.2.4 802.1X, EAP (Extensible Authentication Protocol) 35
5.3 WPA (WIFI PROTECTED ACCESS) 36
5.4 IEEE 802.11I 36
6 NÁVRH A IMPLEMENTACE V RÁMCI ZVOLENÉ SÍTĚ 38
6.1 DŮVODY, CÍLE A PŘÍNOSY ZAVEDENÍ BEZDRÁTOVÉ SÍTĚ NA ISP 38
6.2 OBECNÉ INFORMACE 40
6.2.1 Specifikace Cisco Aironet 1240AG Series 802.11A/B/G 41
6.3 NÁVRH ROZMÍSTĚNÍ BEZDRÁTOVÝCH PŘÍPOJNÝCH BODŮ 42
6.3.1 Instalace bezdrátového přípojného bodu 45
6.4 KONFIGURACE BEZDRÁTOVÉHO PŘÍPOJNÉHO BODU 45
6.4.1 Základní nastavení 46
6.5 NASTAVENÍ KLIENTŮ 48
6.6 KONFIGURACE SÍŤOVÉ TISKÁRNY 51
6.7 MĚŘENÍ DOSTUPNOSTI SIGNÁLU 53
6.8 TESTOVÁNÍ V RÁMCI MOBILNÍ UČEBNY 54
6.8.1 Hardwarové vybavení mobilní učebny 54
6.8.2 Softwarové vybavení mobilní učebny 55
6.8.3 Mobilní počítačová učebna 55
7 ZABEZPEČENÍ SÍTĚ 57
8 ZÁVĚR 59
9 RESUME 60
9.1 RESUME V ČEŠTINĚ 60
9.2 RESUME V ANGLIČTINĚ 61
10 POUŽITÁ LITERATURA: 62
11 PŘÍLOHY 64

1 Úvod

Bezdrátové sítě se objevují po roce 1992. Zařízení bezdrátových sítí pracovala s přenosovými rychlostmi, které nedosahovali ani zlomku rychlosti dnešních bezdrátových sítí. V té době chyběla jakákoli standardizace bezdrátové komunikace, což mělo za následek, že každý výrobce vyráběl vlastní bezdrátové zařízení, které mezi sebou nekomunikovala.

To se změnilo v červenci 1997, kdy byl schválen standard pro bezdrátové sítě IEEE 802.11. Pro tento standard se začalo používat pojmenování WiFi (Wireless Fidelity). Postupem času k původnímu standardu vzniklo a vzniká řada dalších nových norem, doplňků a revizí.

Zavedení standardu, založeném na normě IEEE 802.11, vedlo k velkému rozvoji tohoto odvětví. Kompatibilita jednotlivých zařízení vedla k větší konkurenci mezi výrobci, k postupnému snižování cen a v poslední době také k masivnímu rozšíření WiFi sítí.

Bezdrátové sítě založené na normě 802.11 jsou jen malou podmnožinou sítí označovaných termínem WLAN (Wireless Local Area Network). Patří do rodiny bezdrátových sítí, které využívají jako přenosové médium radiové vlny, podobně jako sítě mobilních operátorů. Všechny tyto sítě mají společný znak, k jejich provozování musí mít provozovatel licenci vydávanou regulačním úřadem. Každý vlastník licence dostává od regulátora přiděleno svoje frekvenční pásmo 2,4 GHz a 5 GHz. To znamená, že každý může provozovat bezdrátovou radiovou síť v bezlicenčním pásmu, pokud dodrží pravidla nastavená regulátorem.

WiFi sítě svým uživatelům nabízí řadu výhod, které přispěly k velkému rozšíření těchto sítí. Mezi základní patří především možnost snadno vytvořit počítačovou síť bez pokládky kabelů. Další výhodou je zavedení jednotného standardu pro WiFi zařízení a použití bezlicenčního pásma.

Tato práce by měla poskytnout základní přehled bezdrátových sítí založených na standardu IEEE 802.11. Je psaná s ohledem na co největší aktuálnost a snaží se jasnou a srozumitelnou formou přiblížit problematiku návrhu a správy bezdrátových sítí pro školu.

2 Cíl práce

Cílem této práce je popsat zásady pro tvorbu bezdrátových sítí, obeznámit se se základními znalostmi a obecnými principy jejich práce, návrhu a správy. Dále je uvedena praktická ukázka konfigurace základních aktivních prvků bezdrátových sítí.

Abychom pochopili bezdrátové sítě, je důležité porozumět jejím technologiím. V úvodu práce jsou popsány základní typy sítí. V další části jsou uvedeny některé základní techniky, které bezdrátové sítě používají. Jejich přehled založený na přenosu radiových vln s podrobným popisem normy IEEE 802.11. Přehled je doplněn seznamem nejdůležitějších norem, které se vztahují ke standardu IEEE 802.11. Další část práce se zabývá hardwarovými komponenty WiFi sítí. V přehledu jsou uvedeny základní aktivní a pasivní prvky, které se při budování WiFi sítí používají.

Další kapitola se zabývá správou WiFi sítí, hlavně správou a konfigurací přístupových bodů, které jsou popsány z hlediska funkčnosti.

Bezpečností WiFi sítí se zabývá další kapitola. Vzhledem k tomu, že WiFi sítě využívají jako svoje přenosové medium radiové vlny, které se šíří vzduchem, jsou mnohem náchylnější na odposlouchávání než jiné typy sítí. Problémy z bezpečností WiFi sítí jsou zásadní a v této kapitole jsou poskytnuty informace, jak lze tyto problémy řešit a odstraňovat.

V následující kapitole se věnuji návrhu sítě a rozmístění přístupových bodů. V závěru práce je kapitola, která se věnuje praktické ukázce konfigurace přístupového bodu a klientského počítače. Kapitola je psaná jako průvodce, podle kterého by neměl být problém nakonfigurovat jakýkoliv přístupový bod a klientský počítač. Dále je zde ukázka konfigurace tiskárny v prostředí bezdrátové sítě a jedna z kapitol je věnována zabezpečení školní bezdrátové sítě. Což je v prostředí školy kapitola velmi důležitá.

3 Počítačové sítě

Počítače umožňují tvorbu dat, grafiky, tabulek atd. Bez počítačové sítě nelze tyto zdroje sdílet. Tento způsob práce se nazývá: „práce v samostatném prostředí“.

Pokud jsou počítače propojené s dalšími počítači a sdílejí společné prostředky, označujeme tuto skupinu jako počítačovou síť. Přitom není podstatné, zda jde o prostředky softwarové nebo hardwarové [1].

Počítače mohou sdílet:

- Data
- Zprávy
- Grafiku
- Faxy
- Tiskárny
- Další hardwarové zdroje

Tento seznam se s růstem informačních technologií neustále rozšiřuje.

3.1 Typy sítí

Počítačové sítě můžeme rozdělit podle mnoha hledisek. Jedním z nich je rozdělení dle rozlehlosti a účelu a to na sítě LAN, MAN, WAN a PAN.

Dále můžeme počítačové sítě rozdělit na sítě typu peer-to-peer a serverové sítě podle role jejich uzlu.

3.1.1 LAN

Lokální sítě propojují koncové uzly typu počítač, tiskárna, server. LAN jsou vždy v soukromé správě a působí na malém území. Připojená zařízení pracují v režimu bez navazování spojení, sdílí jeden přenosový prostředek (drát, radiové vlny), ke kterému je umožněn mnohonásobný přístup.

Přenosové rychlosti LAN začínají na desítkách Mbit/s, nejnovější technologie (r. 2004) umožňují přenos s rychlostí až jednotky Gbit/s.

Mezi lokální sítě patří [21]:

- Ethernet, Fast Ethernet, Gigabit Ethernet (IEEE 802.3)
- Arcnet (už mrtvá technologie)
- Token Bus (IEEE 802.4)
- Token Ring (IEEE 802.5)
- IsoEthernet (IEEE 802.9)
- Bezdrátové sítě (Wi-Fi, IEEE 802.11)
- 100VG-AnyLAN (IEEE 802.12)
- Fiber Distributed Data Interface (FDDI) (ISO/IEC 9314, ANSI X3.x)
- Fibre Channel (ANSI X3.x)

3.1.2 MAN

Sítě typu MAN propojují lokální sítě v městské zástavbě, slouží pro přenos dat, hlasu a obrazu. Metropolitní sítě umožňují rozšíření působnosti lokálních sítí jejich prodloužením, zvýšením počtu připojených stanic a zvýšením rychlosti. Rychlost MAN sítí bývá vysoká a svým charakterem se řadí k sítím LAN. Sítě mohou být jak soukromé, tak veřejné, které provozovatel pronajímá různým uživatelům.

Normalizovaná metropolitní síť existuje jedna[21]:

- protokol Distributed Queue Dual Bus (DQDB) (IEEE 802.6)

3.1.3 WAN

S růstem geografického dosahu sítí přerůstá síť LAN a MAN na WAN (Wide Area Network). Rozlehlé sítě umožňují komunikaci na velké vzdálenosti. Bývají obvykle veřejné, ale existují i soukromé WAN sítě. Typicky pracují prostřednictvím komunikace se spojením, které nepoužívají sdílený přenosový prostředek.

Přenosové rychlosti se velmi liší podle typu sítě. Začínají na desítkách kbit/s, ale dosahují i rychlostí řádu Gbit/s. Příkladem takové sítě může být Internet.

Mezi rozlehlé sítě patří [21]:

- Integrated Services Digital Network (ISDN)
- X25
- Frame Relay
- Switched Multimegabit Data Service (SMDS)
- Asynchronous Transfer Mode (ATM)

3.1.4 PAN [8]

PAN (Personal Area Network) neboli osobní síť je síť, která je tvořena propojením osobních elektronických zařízení jakou jsou například mobilní telefony, PDA, notebooky a další.

Rychlost PAN sítí zpravidla nepřekračuje jednotky Mbit/s. Pro tyto sítě je důležitější odolnost proti rušení, nízká spotřeba a snadná konfigurovatenost [21].

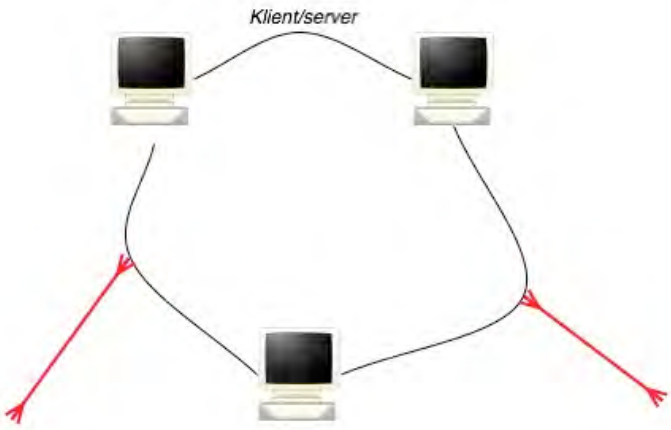
Mezi PAN sítě řadíme:

- Bluetooth
- Zigbee
- IrDA

3.1.5 Sítě typu peer-to-peer

Tyto sítě vycházejí z toho, že všechny počítače zapojené v této síti jsou si rovny. To znamená, že v této síti neexistuje hierarchie počítačů. Všechny počítače fungují jako klient i server. Každý jednotlivý uživatel určuje, která data poskytne ke sdílení, tj. klienti komunikují přímo mezi sebou [1].

V praxi se často využívá specializovaného serveru pro navázání komunikace mezi klienty a tím značné zjednodušení návrhu protokolu sítě. Dnes sítě peer-to-peer zaznamenávají velkou oblibu. Zejména díky tomu, že umožňují snadnou výměnu dat mezi klienty a poskytují svým uživatelům poměrně velkou anonymitu, což pak v mnoha případech vede k nedodržování autorských práv a tím porušování zákona. Jednou ze základních výhod peer-to-peer sítí je fakt, že s rostoucím množstvím uživatelů celková dostupná přenosová kapacita roste, zatímco u modelu client-server se musí uživatelé dělit o konstantní kapacitu serveru, takže při nárůstu uživatelů klesá průměrná přenosová rychlost [8].

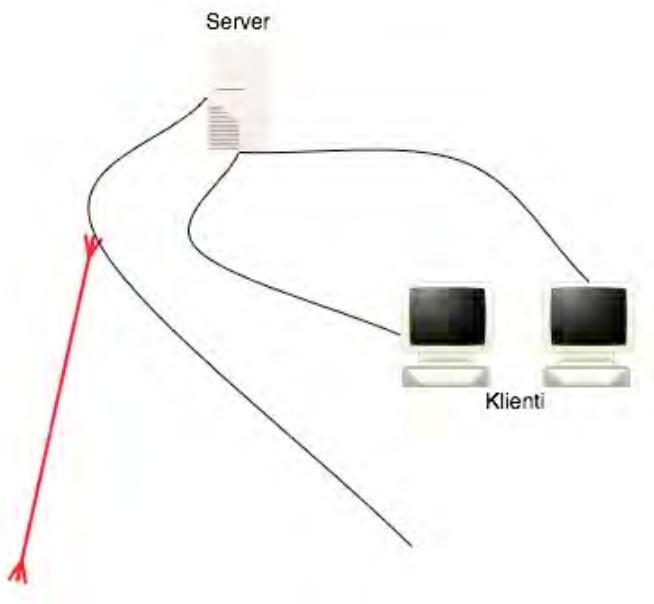


Obrázek č. 1: Síť typu peer-to-peer

Zdroj: vlastní

3.1.6 Serverové sítě

Jsou sítě, kde jeden počítač (nebo více počítačů) je vyhrazen jako server. Takovýto počítač se nepožívá jako klient nebo pracovní stanice, ale je optimalizován na to, aby zajistil rychlé odbavení klientů a zajistil ochranu souborů a adresářů. S rostoucím počtem počítačů připojených v síti roste i počet serverů a následně také jejich specializace, aby jejich úkoly byli provedeni co nejefektivněji [5].



Obrázek č. 2: Serverová síť

Zdroj: vlastní

Základní typy serverů jsou:

- Souborové a tiskové servery – slouží k ukládání souborů a dat
- Webový server – především v síti Internet poskytuje WWW stránky
- Aplikační servery – zpřístupňují klientům serverovou část aplikace
- Poštovní servery – zajišťují posílání elektronických zpráv mezi uživateli sítě
- Komunikační servery – zajišťují posílání zpráv mezi uživateli vlastní sítě a dalších sítí anebo komunikace vlastní sítě se vzdálenými uživateli

Mezi výhody serverových sítí patří centrální správa a kontrola. Další důležitou předností tohoto řešení je možnost zajistit velkou bezpečnost sítě, kterou díky centrálnímu řízení může zajišťovat jeden správce, který stanovuje zásady a pravidla pro všechny klienty sítě [1].

3.2 Bezdrátová síťová komunikace

Pojem bezdrátové síťové komunikace je zavádějící a to především z důvodu, že bezdrátové sítě implikuje síť úplně bez drátů, což ve většině případů neplatí. Většina bezdrátových sítí používá kabely k propojení bezdrátových komponent, částí svých segmentů a kabelové sítě. Takovéto kombinované sítě se také nazývají hybridní sítě [1].

3.2.1 Přenosové techniky

Pro přenos dat se u bezdrátových zařízení používají různé techniky. Následující přehled obsahuje některé z nejvýznamnějších technik bezdrátové komunikace.

Infračervené zařízení, IrDA

IrDA (Infrared Data Association) je organizace definující standardy komunikačních protokolů pro infračervená záření. Tato technologie umožňuje snadnou komunikaci mobilních zařízení na krátkou vzdálenost. Používá se pro komunikaci s mobilními telefony, palmtopy atp. Komunikace pomocí IrDA vyžaduje přímou viditelnost, dosah je cca 1 metr a přenosové rychlosti se pohybují od 2,4 Kbit/s až 16 Mbit/s [7].

Laser

Pro komunikaci pomocí laseru se dnes využívá dvousměrných teleskopů s rychlými transceivery, které mohou dosáhnout rychlosti až 2,5 GB/s. Provozovatel musí při použití této technologie zajistit přímou viditelnost mezi optickými jednotkami. Sníh ani déšť nemají na funkčnost a spolehlivost těchto linek vliv, avšak fatální následky na funkčnost má mlha [22].

Radiové frekvence

Technologie založené na komunikaci pomocí radiových vln patří mezi nejrozšířenější a nejvíce využívané. Radiové přenosy mohou probíhat na vzdálenost několika stovek až tisíce metrů a není omezena přímou viditelností.

3.2.2 Přehled bezdrátové radiové technologie

Frekvence

Bezdrátové sítě využívající radiové vlny pracují ve stanovených frekvencích. Používání radiofrekvenčních pásem podléhá regulaci ze strany státních úřadů. Většina pásem vysílacího spektra podléhá licencím, například ty, co využívají provozovatelé k televiznímu a rozhlasovému vysílání nebo spektrum, které využívají mobilní operátoři.

Proto musí WiFi sítě využívat jednoho ze dvou nelicencovaných pásem: [2]

- 2,4 GHz v pásmu 2,412 – 2,472 GHz (1-13 kanálů, Evropa mimo Francii a Španělska)
- 5 GHz v pásmu 5,15 – 5,725 GHz (1-79 kanálů, Evropa)

Pásmo 5 GHz je velmi nepřehledné, má několik subpásem, které mají rozdílnou regulaci [13].

Spektrum

Ve frekvenčním pásmu 2,4 a 5 GHz není potřeba žádná licence, Český Telekomunikační Úřad přesto zavádí určitou regulaci. Tato regulace má zabránit, aby bezdrátové přenosy nevyužívali nadměrnou šířku pásma a nepoužívali příliš velký výkon vysílání. To by mohlo způsobovat rušení jiných signálů, které využívají tyto pásma. Další pravidlo, které ČTÚ vyžaduje, je používání jedné ze tří technologií rozprostřeného spektra [2].

Rozprostřené spektrum

Základní myšlenkou rozprostřeného spektra je, že se signál rozprostře po širokém rozsahu frekvencí. Rozprostření signálu vede k tomu, že je méně citlivý k rušení a snižuje jeho citlivost k interferencím a v podstatě vede k neefektivnímu využití kmitočtového pásma. Na druhou stranu tak zajišťuje spolehlivější přenosy. V podstatě toto řešení preferuje spolehlivost před efektivitou [2].

Technologie rozprostřeného spektra

DSSS (Direct Sequence Spread Spectrum) Rozprostřené spektrum v přímé posloupnosti rozprostírá signály přes několik kanálů v určitém frekvenčním rozsahu. Binární řetězec nazvaný kód prostředí vytváří redundanci. Signál je rozprostřen do většího radiového spektra, je méně citlivý vůči rušení, což zajišťuje větší spolehlivost signálu. [2].

FHSS (Frequency Hopping Spread Spectrum) Rozprostřené spektrum s přeskakováním mezi frekvencemi. Tato technologie využívá k přenosu datové zprávy a přeskoky mezi mnoha nosnými frekvencemi. Vysoké spolehlivosti je dosaženo díky tomu, že nepotvrzené (tj. chybné přenosné rámce) jsou přeneseny znovu s jinou nosnou frekvencí. Další výhodou je možnost umístění více systémů v jednom místě, použitím různých frekvencí v každém systému [2].

OFDM (Orthogonal Frequency Division Multiplexing) Ortogonální multiplex s kmitočtovým dělením využívá toho, že rozděluje dostupné spektrum na podkanály a vysílá část daného datového přenosu přes každý podkanál, což zvyšuje odolnost proti interferenci. OFDM se používá mimo jiné pro přenos signálu v ADSL, bezdrátových sítích standardu IEEE 802.11a/g a standardech pro digitální televizi DAB a DVB-T [2].

MIMO (Multiple-input multiple-output), česky více vstupů více výstupů, je abstraktní matematický model pro multi-anténní komunikační systémy. Během posledních let se výrazněji používá MIMO technologie v oblasti bezdrátové komunikace pro významný nárůst datové propustnosti a dosahu při zachování šířky pásma a celkového výdeje vyzařovací energie [2].

MIMO bezdrátová komunikace využívá fenoménu vícecestné propagace k zvýšení propustnosti a dosahu nebo k snížení počtu přenosových bitových chyb, místo snahy o eliminaci efektu vícecestné propagace, o kterou se snaží tradiční Single-Input Single-Output [23].

IEEE 802.11

The Institute of Electrical and Electronic Engineers (IEEE) sdružuje přes 350 000 elektroinženýrů a informatiků v cca 150 zemích všech světadílů. Tato organizace vyvíjí a schvaluje normy pro širokou řadu počítačových technologií. Skupiny expertů navrhují nové normy, podle kterých pak výrobci vyvíjejí své výrobky. Číslo 802 slouží pro označení všech síťových norem, další číslo označuje podskupinu síťových norem (např. číslo .11 slouží pro označení norem pro bezdrátové sítě).

První norma s označením IEEE 802.11 byla přijata v roce 1997. Jednalo se o radiovou normu pracující v pásmu 2,4 GHz s maximální propustností 2 Mbit/s. Norma byla dále zmodernizovaná a dostala označení 802.11 High Rate a dosahovala přenosových rychlostí až 11 Mbit/s. V roce 1999 došlo k dalšímu přejmenování této normy na 802.11b. Dále vznikla další norma s označením 802.11a, která přinesla vyšší rychlost, odlišnou metodu rozprostřeného spektra a pracovala ve frekvenčním pásmu 5 GHz. V roce 2002 přibyla další norma 802.11g. IEEE poté schválilo další normu v oblasti bezdrátových lokálních sítí. Nejednalo se o čtvrtý typ, ale o doplněk ke specifikaci 802.11a určenou pro použití v Evropě [2].

Přehled základních norem 802.11

802.11b

Norma IEEE 802.11b je v podstatě vylepšená původní norma IEEE 802.11. O rychlé rozšíření této normy se postarala firma Apple Computer, která jako první zavedla dostupné výrobky založené na této normě. V roce 1997 ji uvedla pod názvem AirPort. Sada se skládala z bezdrátového přístupového bodu a PC karty pro notebook Macintosh. Díky tomu se bezdrátová technologie značně zpopularizovala a rozšířila. Dnes patří norma 802.11b mezi nejrozšířenější z hlediska dostupnosti zařízení založených na této normě a oblíbenosti mezi uživateli [2].

Sítě založené na této normě pracují s maximální přenosovou rychlostí 11 Mbit/s a využívají rozostřeného spektra DSSS.

802.11a

Norma IEEE 802.11a byla schválena brzy po normě 802.11b v roce 1999. Práce na této normě začali sice již dříve, ale vyžádali si delší čas vzhledem ke složitějšímu přenosu na fyzické vrstvě.

Norma pracuje na frekvenčním pásmu 5 GHz, teoretická přenosová rychlost je 54 Mbit/s a používá metodu rozprostřeného spektra OFDM. Výhodou této normy je, že využívá pásmo 5 GHz, které nabízí na rozdíl od často přeplněného pásma 2,4 GHz větší šířku a poskytuje více kanálů pro bezdrátovou komunikaci [2].

802.11g

Norma IEEE 802.11g byla schválena v roce 2002. Maximální rychlost bezdrátových sítí založených na této normě je 54 Mbit/s, používá technologii rozprostřeného spektra OFDM a pracuje ve frekvenčním pásmu 2,4 GHz. Další důležitou vlastností je zpětná kompatibilita s rozšířenou normou 802.11b [2].

802.11n

IEEE 802.11n je WiFi standard, který si klade za cíl upravit fyzickou vrstvu a podčást linkové vrstvy, takzvanou Media Access Control (MAC) podvrstvu tak, aby se docílilo reálných rychlostí přes 100 Mbit/s. Nicméně maximální rychlost může být až 540 Mbit/s. Měl by se také zvýšit dosah [24].

Zvýšení rychlosti se dosahuje použitím MIMO (multiple input multiple output) technologie, která využívá vícero vysílacích a přijímacích antén [24].

Standard	**Rok vydání**	**Pásmo [GHz]**	**Maximální Rychlost [Mbit/s]**	**Fyzická vrstva**
původní IEEE 802.11	1997	5	54	OFDM
IEEE 802.11a	1999	5	54	OFDM
IEEE 802.11b	1999	2,4	11	DSSS
IEEE 802.11g	2003	2,4	54	OFDM
IEEE 802.11n	2007	2,4 nebo 5	540	MIMO

Tabulka č 1: Přehled základních norem standardu 802.11

Zdroj: [20]

Doplňující normy 802.11

802.11e

Tato norma zavádí podporu QoS (Quality of Service). QoS zajišťuje kvalitu hovorového a obrazového signálu. To by mělo umožnit realizovat přenosy citlivé na ztrátu paketů, jako jsou videokonference, multimediální přenosy, internetové telefonování atp. Tato norma nebyla dosud schválena [20].

802.11f

V roce 2003 byla schválena norma IEEE 802.11f, která zavedla protokol IAPP (Inter-Access Point Protocol), který umožňuje spolupráci přístupových bodů od různých výrobců a vylepšuje mechanizmus předávání stanic mezi dvěma radiovými kanály z jedné sítě do sousední s připojením k jinému přístupovému bodu tzv. roaming [20].

802.11h

Tato norma zavádí použití dynamického výběru kanálů DCS (Dynamic Channel Selection) a ř ízení vysílacího výkonu TPC (Transmit Power Control) u zařízení pracujících v kmitočtovém pásmu 5 GHz. Norma byla schválena v roce 2003 [20].

802.11i

Norma 802.11i zavádí nové bezpečností mechanismy do hlavních norem 802.11a/b/g. Odstraňuje především známé problémy se slabým zabezpečením a snaží se tak standard 802.11 udělat zajímavým i pro firemní zákazníky, pro které byla slabá bezpečnost těchto sítí velkým problémem [20].

Bluetooth

Bluetooth je bezdrátová radiokomunikační technologie pracující ve frekvenčním pásmu 2,4 GHz a používá rozprostřené spektrum FHSS. Technologie Bluetooth je definovaná standardem IEEE 802.15.1 a spadá do kategorie osobních počítačových sítí PAN. Existuje několik verzí, které se liší dosahem a rychlostí přenosu. Verze 1.1 s maximálním dosahem 10 metrů a verze 1.2 s dosahem 100 metrů. Verze 1.2 se používá v drtivé většině současných zařízení využívajících Bluetooth. Datová propustnost se pohybuje okolo 1 Mbit/s. V současné době se připravuje nová specifikace Bluetooth 2.0 ERD, která by měla přenosové rychlosti zvýšit až na trojnásobek současného maxima [2].

HiperLAN

HiperLAN (High Performance Radio Local Area Network) byl vyvinut evropskou společností BRAN v rámci Evropského ústavu pro normalizaci telekomunikací (ETSI). Existuje ve dvou verzích HiperLAN/1 a HiperLAN/2. Obě pracují ve frekvenčním pásmu

5 GHz a dosahují přenosových rychlostí v případě starší verze 24 Mbit/s a v případě novější verze 54 Mbit/s [2,9].

Na rozdíl od sítí 802.11 HiperLAN podporuje kvalitu služeb pro přenos hovorových signálů a videa tzv. QoS, poskytuje také kvalitní zabezpečení, efektivně řídí spotřebu energie a umožňuje snadnou konfiguraci [2,9].

WiMax

WiMax (Worldwide Interoperability for Microwave Access) představuje bezdrátovou technologii určenou pro spojení na dlouhou vzdálenost a umožňuje vysokou datovou propustnost. WiMax je definován na standardu IEEE 802.16. Tento standard se začal vyvíjet od roku 1998, ale většina prací proběhla v roce 2000 až 2003. Cílem tohoto standardu je vytvořit snadný a levný způsob širokopásmového připojení k internetu pro metropolitní sítě.

Mezi důležité vlastnosti standardu 802.16 patří podpora systému řízení kvality služeb QoS, jež je zabudován do MAC vrstvy a poskytuje diferenciaci nabízených služeb.

Na standardech WiMax se neustále pracuje a tak v nejbližší době by se uživatelé těchto sítí měli dočkat také mobilních zařízení na tomto standardu v podobně přídavných karet do notebooku atp. Zařízení založené na technologii WiMax tak mají šanci stát se postupem času vhodným doplňkem WiFi sítí, tam kde je potřeba propojení na delší vzdálenosti. V tomto ohledu se jeví budoucnost WiMaxu jako velmi slibná [10].

3.2.3 WiFi

WiFi (Wireless Fidelity) Aliance pro kompatibilnost bezdrátového ethernetu (WECA v roce 2003 přejmenována na WiFi Alliance) přijala označení WiFi jako značku pro produkty kompatibilní se standardem IEEE 802.11. WECA byla založena především dodavateli výrobků za účelem podpory standardu 802.11 a z důvodu certifikačního programu, který má zajistit vzájemnou kompatibilitu výrobku od různých výrobců mezi sebou. WiFi Alliance testuje výrobky a těm, které splňují dané požadavky, dává certifikaci a svolení k používání loga na jejich zařízení a marketingových materiálech. Logo WiFi představuje záruku toho, že takto označené výrobky by neměl být problém propojit mezi sebou [10].

Obrázek č. 3: Logo WiFi Alliance zaručuje kompatibilitu. Barevné oválné značky s písmenky zpřesňují, které standardy zařízení splňuje

Zdroj:[12]

Termín WiFi se v poslední době používá pro označení všech sítí založených na standardu IEEE 802.11, což není přesné (ne všechna zařízení musí vyhovovat podmínkám WiFi Alliance), ale je to vžité natolik, že je to chápáno jako ekvivalent k sítím standardu IEEE 802.11 a/b/g/n [2].

3.3 Podrobný popis IEEE 802.11

Při stavbě sítí založených na normě 802.11 je důležité tuto normu pochopit. Pomůže nám to při posuzování (ne)výhod, které sítě WiFi nabízejí.

Základní součásti WiFi sítě

Základem všech WiFi sítí jsou síťové stanice, které jsou tvořeny síťovým adaptérem nainstalovaným nebo připojeným k počítači. Síťový adaptér obsahuje radio přijímač/vysílač a většinou také anténu, která slouží k zesílení radiového signálu. Další prvek většiny bezdrátových sítí je přístupový bod neboli AP (Access Point). AP prodlužuje dosah sítě a zpravidla i řídí její provoz. AP je vybaven radiovým zařízením podobně jako síťová stanice.

Aby WiFi stanice a přístupové body mezi sebou úspěšně komunikovali, musí využívat stejnou normu pro komunikaci, nebo normy mezi sebou navzájem kompatibilní. [2]

3.3.1 IEEE 802.11 a model OSI

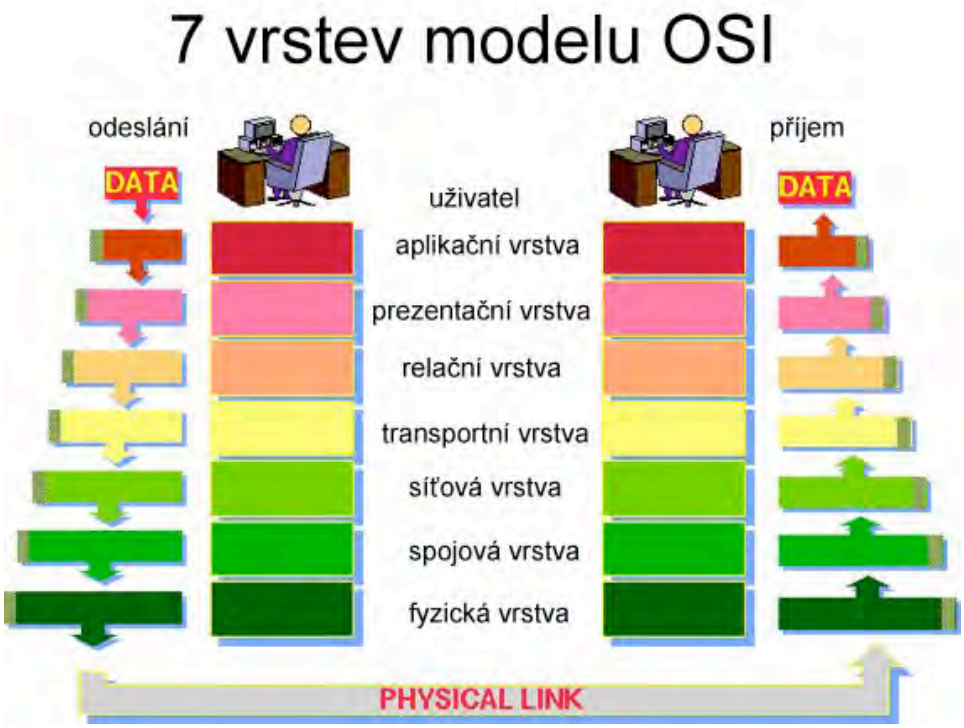
OSI (Open System Interconnection) je sedmivrstvý model, který popisuje strukturu sítě a průběh komunikace od nejnižší vrstvy (fyzická vrstva) po nejvyšší (aplikační vrstva). Model OSI je hierarchický, každá ze sedmi vrstev má jasně definované funkce potřebné pro komunikaci a využívá pro svou činnost sousední nižší vrstvy. Ne všechny vrstvy referenčního modelu OSI musí být aktivní. Pokud existuje vrstva, která je vynechána nazývá se nulová nebo transparentní [2].

Komunikace mezi vrstvami se řídí pravidly, která se nazývají rozhraní a komunikace mezi vrstvami různých systémů se řídí protokoly. Normy IEEE 802 pracují na fyzické a síťové vrstvě jako 802.3 (běžně označované jako Ethernet) a 802.11 (bezdrátový protokol - WiFi).

Protokoly vyšších vrstev referenčního modelu jsou např. TCP/IP, NETBIOS atd. Tyto protokoly jsou nezávislé na nižších vrstvách a používají tyto nižší vrstvy jako platformu, na které pracují. Vrstvy se často člení do podvrstev, které přebírají jen určitou část práce vrstvy [2].

Vrstvy ISO/OSI [3]

- Fyzická vrstva (physical layer) – komunikace na nejnižší hardwarové úrovni
- Spojová vrstva (data-link layer) – kódování a přenos informací
- Síťová vrstva (network layer) – obsluha přenosových tras a zpráv
- Transportní vrstva (transport layer) – řízení doručování informací a kvality
- přenosu
- Relační vrstva (session layer) – udržování a koordinace komunikace
- Prezentační vrstva (presentation layer) – formátování, konverze a zobrazování
- přenesených dat
- Aplikační vrstva (application layer) – přenos informací mezi programy



Obrázek č. 4: model OSI

Zdroj:[13]

3.3.2 Topologie bezdrátové sítě

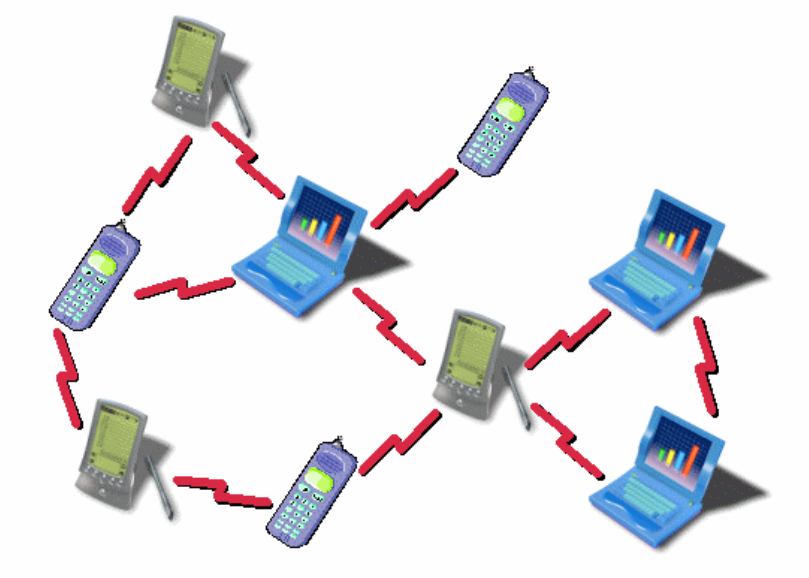
Pro označení základního uspořádání bezdrátové sítě se používá termín topologie. Jedná se o fyzické uspořádání počítačů a dalších síťových zařízení v síti.

Bezdrátovou síť lze nastavit dvěma způsoby:

- IBSS (Independent Basic Service Set) klienti se připojují sami mezi sebou
- BSS/ESS (Basic Service Set/Extended Service Set) klienti se připojují k přístupovému bodu

IBSS

IBSS je též označován jako Ad-hoc režim. Pracuje tedy v režimu peer-to-peer to znamená, že ke své č innosti nepotřebují zařízení v síti přístupový bod. Tento režim je vhodný zejména pro dočasné propojení počítačů, nebo pro sítě kde je malý počet bezdrátových klientů. Nevýhodou tohoto řešení je slabá bezpečnost [2,5].



Obrázek č. 5: Ad-hoc síť

Zdroj:[14]

BSS/ESS

BSS/ESS též označovaný jako infrastrukturní síť [2].

BSS je základní soubor služeb pro sítě skládající se ze zařízení která jsou ve vzájemném dosahu nebo v dosahu přístupového bodu [2].

ESS jsou sítě s rozšířeným souborem služeb, které umožňují překrývání přístupových bodů. To rozšiřuje dosah jedné sítě [2].

Obrázek č. 6: Infrastrukturní síť

Zdroj: [14]

3.4 Hardwarové vybavení bezdrátových sítí

3.4.1 Přístupový bod (Access Point)

Access Point neboli přístupový bod je zařízení, ke kterému se připojují klienti. AP zajišťuje přístup bezdrátových zařízení v lokální síti, přístup na internet, most mezi bezdrátovými zařízeními a kabelovými sítěmi atp.

Většina přístupových bodů má jednu nebo více antén. Všechny přístupové body jsou z hlediska své vnitřní struktury stejné. Každý bod obsahuje minimálně jeden radio přijímač/vysílač pracující na určité frekvenci podle norem 802.11, programové vybavení pro řízení přístupového bodu a bezdrátové sítě, porty pro připojení přístupového bodu ke kabelové síti (LAN port) a k internetu (WAN port) [2].

Obrázek č. 7: Access Point

Zdroj: [15]

Radiostanice

Přístupový bod obsahuje alespoň jednu radiostanici. Tato radiostanice určuje, kterou normu bezdrátové komunikace zařízení podporuje. V současné době patří mezi nejrozšířenější norma 802.11b (11 Mbit/s) [2].

Komunikační porty

Přístupový bod obsahuje zpravidla ethernetový WAN port pro připojení na internet. Dále obsahuje jeden nebo více LAN portů k připojení lokální sítě [2].

Antény

Součástí přístupových bodů je jedna nebo více antén, které umožňují komunikaci zařízení. K přístupovému bodu můžeme připojit také externí anténu pro zvětšení dosahu [2].

3.4.2 Softwarový přístupový bod

Softwarový přístupový bod je počítač vybavený softwarem pro směrování (routování), obsahující jeden nebo více WiFi adapterů, ethernetový adaptér a většinou je vybavený switchem pro připojení do lokální sítě.

3.4.3 Síťový most

Síťový most (bridge) slouží ke spojení dvou segmentů sítě. Díky těmto mostům mohou dva segmenty LAN sítě pracovat jako jediná síť. Mnoho výrobců funkci síťových mostů integruje do svých přístupových bodů [2].

3.4.4 Bezdrátový opakovač

Bezdrátový opakovač přijímá signál od zdroje, zesílí ho a dále ho pošle do cílového místa. Opakovače se používají tam, kde je potřeba rozšířit oblast pokrytí bezdrátové sítě [2].

3.4.5 WiFi síťový adaptér

Součásti síťového adaptéru

Každý adaptér obsahuje radiostanici a konektor, který odpovídá jednomu vstupnímu nebo výstupnímu portu počítače. Síťové adaptéry často obsahují malou anténu pro zvýšení dosahu anebo konektor pro připojení externí antény.

Druhy síťových adaptérů

PCI síťové adaptéry

Tyto adaptéry jsou určeny pro stolní PC, komunikace probíhá přes PCI sběrnici. Těmito zařízeními lze vybavit jakýkoliv stolní počítač. Většina těchto rozšiřujících karet má výstup pro externí anténu. V dnešní době čím dál víc výrobců integruje WiFi síťové adaptéry do základních desek [2].

Obrázek č. 8: PCI bezdrátová karta

Zdroj: [16]

PCMCIA karty

Dnešní notebooky obsahují jeden nebo více PCMCIA slotů pro PC karty typ II. Většina těchto karet jsou typu II. Výhodou karet do PCMCIA slotu je jejich snadná instalace, kompaktní rozměry a cena. Lze je použít v noteboocích a v zařízeních vybavených PCMCIA slotem [2].

Obrázek č. 9: PCMCIA karta

Zdroj: [16]

USB síťové adaptéry

USB adaptéry se připojují k počítači přes sběrnici USB. Touto sběrnicí je dnes vybaven každý počítač či notebook. Díky snadné dostupnosti USB jsou tyto adaptéry dnes nejrozšířenější. Nevýhodou tohoto adaptéru je, že v naprosté většině nejsou vybaveny žádným konektorem pro připojení externí antény [2].

Obrázek č. 10: USB WiFi klient

Zdroj: [16]

3.4.6 Antény

Antény zvyšují dosah a pokrytí WiFi sítí. Antény pouze zaostřují vyzařovanou energii do určitého směru, signál nezesilují.

Síťové adaptéry a přístupové body se dodávají s anténami. U notebooků jsou antény integrované [2].

K většině přístupových bodů a síťových adaptérů je možné připojit externí antény, které nahrazují antény dodávané výrobci zařízení jako součást balení. To umožňuje zvýšit dosah přístupových bodů až na několik kilometrů při vhodném umístění antény [2].

Charakteristické vlastnosti antén [2]:

Šířka frekvenčního pásma (bandwidth) – Jedná se o frekvenční pásmo (např. 2,4GHz pro normy 802.11b/g). Každá anténa je díky své velikosti vhodná pro konkrétní frekvenci.

Zisk (gain) – Popisuje stupeň směrovosti antény. Směrové antény směřující signál přímočaře mají větší zisk než antény, které distribuují signál v širším diagramu. Zisk se měří v decibelech dB a počítá se podle vzorce 10log(výstupní výkon/vstupní výkon). Zisk tedy představuje poměr dvou výkonů a udává se většinou v dBi (vztaženo k izotropní anténě). Zisk antény vyjádřený v dBi je porovnání zisku antény s izotropní anténou, což je teoretická anténa s nulovým ziskem/ztrátou. Zisk se také může vztahovat k jednomu miliwattu, pak je vyjádřený v dBm.

Odstup signálu od šumu S/N (signal to noise) – Vyjadřuje sílu radiového signálu vzhledem k šumu v daném prostředí, měří se v decibelech dB.

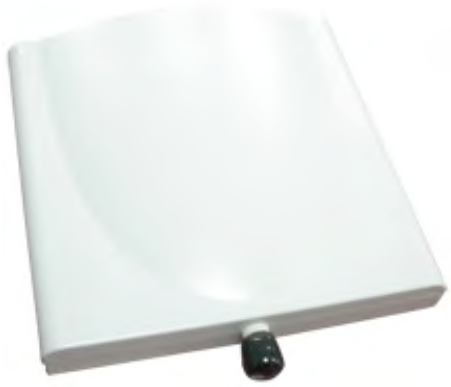
Vyzařovací diagram (radiation pattern) - Slouží pro označení diagramu vyzařovaní antén v prostoru. Směrové antény provádějí modulaci lineárně ve směru zaměření antény, naopak všesměrové antény pokrývají kruhový prostor.

Úhel vyzařování (beam width) – Úhel vyzařování se vyjadřuje ve stupních a vztahuje se obvykle k vodorovné rovině. Úhel vyzařovaní, lze použít pro výpočet oblasti pokrytí signálem.

Polarizace (polarization) – Elektromagnetické vlny lze vysílat buď s vertikální, nebo s horizontální polarizací. Polarizace antén mezi vysílačem a přijímačem musí být stejná, aby se předešlo vytváření signálového šumu a ztrátám anténního zisku.

Typy antén

Výběr antény závisí na jejím použití. Na výběr jsou jak malé antény vhodné zejména k notebookům, tak velké antény určené pro montáž na střechy. Výběr antény je vždy určitým kompromisem mezi oblastí pokrytí a sílou signálu.



Obrázek č. 12: Směrová anténa

Zdroj: [17]

Obrázek č. 13: Všesměrová anténa

Zdroj: [17]

Všesměrové antény

Jak je z názvu patrné, všesměrové antény vyzařují signál všemi směry. Obvykle jsou tyto antény sloupcového tvaru a umísťují se ve vertikální poloze. Výhodou těchto antén je, že pokrývají velkou oblast a jsou vhodné tam, kde jsou zařízení rozprostřena v kruhovém prostoru. Čím větší zisk má všesměrová anténa, tím plošší signál vyzařuje. Nevýhodou

tohoto typu antén je, že v bezprostřední blízkosti a pod úrovní této antény se nalézá mrtvé místo [2].

Sektorové antény

Jsou obdobou všesměrových antén. Jejich úhel vyzařování je na rozdíl od nich maximálně 180 stupňů. Jelikož jsou sektorové antény směrovější, dosahují tak většího zisku a jsou méně citlivé na šum. Sektorové antény jsou vhodné tam, kde zařízení leží v jednom směru [2].

Yagi antény

Tyto antény jsou určeny pro propojení přístupových bodů na delší vzdálenosti. Yagi antény mají úhel vyzařování 15-60 stupňů a poskytují vyšší zisk než sektorové antény [2].

Parabolické antény

Parabolické antény jsou vhodné pro venkovní instalaci. Dosahují největších zisku a jsou vysoce směrové, a proto se hodí k propojení přístupových bodů na velké vzdálenosti [2].

3.4.7 Konektory a kabelová vedení

Kabely se ve WiFi sítích používají k propojení antény s přístupovým bodem nebo síťovým adaptérem. Při výběru kabelu pro WiFi síť je nutné vybrat správný a to především z hlediska jeho použití, výběrem nevhodného kabelu může dojít k útlumu signálu a dosahu antény.

Koaxiální kabel je zdrojem útlumu, čím delší kabel použijeme, tím větší útlum způsobí. Na krátké vzdálenosti (do 10 metrů) je vhodné použít tenké kabely s průměrem 5 mm, jejich útlum je okolo 0,5 dB/m. Jejich velkou výhodou je široká dostupnost konektorů (např. RSMA konektory, TNC, SMA atd.).

Pro delší vzdálenosti a venkovní použití jsou vhodnější koaxiální kabely s průměrem 11 mm. Dosahují nižšího útlumu okolo 0,22 dB/m a tak se mohou použít i na delší vzdálenost. Mají také kvalitnější dielektrikum, a proto jsou odolnější proti rušení.

Koaxiální kabely se vedou co nejkratší cestou, bez prudkých ohybů, kroucení a smyček. Kabel se nesmí namotávat na kovové trubky ani stožáry a nesmí se ani vést uvnitř těchto stožárů, nepoužívají se kovové průchodky [3].

Podobně jako kabely tak i konektory představují ztrátu signálu. Používají se konektory typu SMA, TNC a N. Typ konektoru musí také odpovídat konektoru dané antény a mít opačnou polaritu [3].

4 Správa sítí

4.1 Správa a konfigurace přístupového bodu

Přístupový bod umožňuje správu a konfiguraci pomocí konfiguračního softwaru.

4.1.1 Možnosti konfigurace přístupových bodů [3]

SNMP (Simple Network Management Protocol) označuje protokol a standard zpřístupňující dohodnuté postupy, pravidla a architekturu pro management sítí TCP/IP nebo IPX a jejich síťové prvky. Vyžaduje znalosti terminologie a není tak uživatelsky přátelský oproti klientskému softwaru.

Webové rozhraní je dnes nerozšířenější způsob konfigurace přístupových bodů. Webový prohlížeč je standardní součástí každého operačního systému, umožňuje snadnou konfiguraci a správu přístupového bodu.

Telnet ocení uživatelé, kteří vyžadují dálkovou správu přístupových bodů.

4.1.2 Přístup na internet [2, 3]

Přístupový bod umožňuje sdílení připojení na internet. Způsoby jakými se přístupový bod autorizuje a konfiguruje do sítě internet je následující:

Automatické získání IP adresy. Přístupový bod si vyžádá IP adresu od serveru a tu si nechá, dokud se od internetu neodpojí

Statická IP adresa. Poskytovatel internetového připojení přidělí permanentní veřejnou IP adresu.

PPPoE (Point-to-Point over Ethernet) neboli dvoubodový protokol přes ethernet. Toto připojení využívají někteří poskytovatelé internetu pro připojení DSL nebo kabelových uživatelů k jejich síti.

PPTP (Point-to-Point Tunneling Protocol) používá se pro připojení k ADSL lince.

DHCP (Dynamic Host Configuration Protocol) přístupový bod může získat IP adresu pro sebe od poskytovatele internetu namísto použití statické IP adresy.

4.1.3 DHCP server

DHCP server poskytuje počítačům přístup na síť přes TCP/IP protokol. Každému počítači na síti přiřazuje IP adresu dynamicky. IP adresa slouží k jeho identifikaci. V kombinaci s překladem síťových adres NAT (Network Address Translation), který umožňuje, aby

několik počítačů sdílelo jednu veřejnou IP adresu. Všechny počítače propojené do sítě tak mohou využívat jednu veřejnou IP adresu přiřazenou od poskytovatele internetu.
DHCP server je standardním vybavením přístupových bodů, a většina jich obsahuje i NAT [2].

4.1.4 Veřejné a privátní IP adresy

Veřejné IP adresy přiděluje poskytovatel internetového připojení a slouží k jednoduché identifikaci na internetu. Privátní IP adresy se používají k identifikaci počítače v lokální síti a nejsou na internetu rozeznávány. Pokud chceme připojení k internetu sdílet, musíme za jednu veřejnou IP adresu, kterou dostaneme od poskytovatele internetového připojení schovat lokální síť. K sdílení veřejné IP adresy slouží směrovací funkce přístupového bodu NAT. DHCP server přiřadí každému počítači v lokální síti privátní IP adresu a sám se připojí na internet pomocí veřejné IP adresy. Přístupový bod tak předává internetové pakety počítačům na lokální síti. Všechny počítače jsou pak připojeny přes jednu veřejnou IP adresu [2].

4.1.5 Firewall [2]

Firewall chrání počítač před vnějším napadením a nežádoucím průnikům do sítě z internetu. Tuto č innost vykonává blokováním prostředků, které využívají specifické internetové a síťové aplikace.
Internetové aplikace (např. elektronická pošta, web FTP atd.) používají pro komunikaci takzvané komunikační porty. Každá aplikace má pro svoji komunikaci přiřazeny čísla portů, které používají pro svoji komunikaci. Každý port má své číslo (například webový prohlížeč používá port 80, FTP používá port 21 atd.).
Jestliže je port na počítači otevřen může s ním navázat komunikaci kdokoliv, kdo zná IP adresu daného počítače. Mohou komunikovat buď pomocí aplikace, která je k tomuto účelu určená, nebo pomocí speciálního softwaru, který umí detekovat otevřené porty. Případný útočník může prostřednictvím těchto nástrojů do počítače proniknout.
Firewall umožňuje zablokovat všechny nestandardní porty, které uživatel nepotřebuje a tak chránit počítač před nežádoucími návštěvníky. Také umožňuje nastavit přístup na určité porty nebo jen z určitých portů.
Firewall přístupového bodu chrání síť proti průnikům z internetu prostřednictvím blokování komunikace, která přichází z portu WAN (vnější síť). Počítače, které jsou připojeny za tímto firewallem tedy na lokální síti (vnitřní síť) jsou chráněny

prostřednictvím firewallu proti průnikům z internetu, ale komunikace na úrovni lokální sítě probíhá bez omezení.

Firewall přístupového bodu neobsahuje tolik funkcí jako softwarový firewall. Softwarový firewall nabízí mnoho dalších doplňkových služeb a funkcí. Je vhodné nespoléhat se jen na firewall přístupového bodu a lze proto doporučit instalaci softwarového firewallu na všech počítačích.

4.1.6 DMZ – demilitarizovaná zóna

Demilitarizovaná zóna umožňuje, aby byl počítač, který je ve vnitřní síti viditelný a přístupný z internetu bez ochrany firewallu. V tomto nastavení bude přístupový bod směřovat veškerou komunikaci na počítač v DMZ bez kontroly a omezení. Toto nastavení se používá při provozu webových či mailových serverů [2].

4.1.7 Přesměrování portů

Přesměrování portů (Port forwarding) představuje možnost, jak na vnitřní síti provozovat služby dostupné z internetu. Přesměrování portů umožní vybrat jeden nebo více počítačů a jeden nebo více portů, které budou k dispozici pro vnější síť, zatímco zbývající část vnitřní sítě zůstane chráněna. Počítač, na který je provoz přesměrován, musí mít nastavenou statickou IP adresu. Přesměrování využívají například on-line hry, IP telefonie, peer-to-peer klienti [2].

4.1.8 Filtrování

Řada přístupových bodů umožňuje filtrování služeb a přístup na internet. Pomocí filtrů můžeme blokovat určité servery, omezit přístup na základě klíčových slov nebo zdrojové domény, omezit přistup v určitých hodinách a na určité porty [2].

4.1.9 VPN (Virtual Private Network)

Virtuální privátní síť umožňuje počítačům připojeným k internetu bezpečně přistupovat k prostředkům privátní sítě. K privátní síti přistupuje počítač prostřednictvím internetu, přičemž dochází k šifrování všech dat přenášených ze vzdáleného počítače na privátní síť. Tato služba umožňuje, aby zaměstnanci využívali privátní sít i když se nacházejí mimo kancelář.

VPN zajišťuje větší bezpečnost přenášených dat než bezpečnostní mechanizmy normy 802.11. Mezi nejpoužívanější protokoly patří PPTP a L2TP. U správce sítě je nutné si ověřit, jaký druh přístupu síť podporuje [5].

5 Bezpečnost sítí

Bezdrátová síť má jednu velkou nevýhodu, vycházející z principu komunikace těchto sítí. Na rozdíl od kabelových sítí na to, aby někdo mohl odposlouchávat komunikaci, stačí zachytit vysílaný signál.

Pomocí dalších nástrojů nebo programů volně dostupných na internetu může útočník snadno zachytávat hesla a další citlivá data.

Mezi další bezpečnostní rizika bezdrátových sítí patří zabránění neautorizovanému přístupu do sítě.

Bezpečnost bezdrátových sítí lze rozdělit do dvou hlavních skupin:

- Šifrování – zabezpečení přenášených dat proti odposlechnutí
- Autentizace – zabezpečení proti neoprávněnému přístupu

5.1 Šifrování

5.1.1 WEP (Wired Equivalent Privacy)

Většina bezdrátových sítí pro své zabezpečení používá WEP. Jedná se o standard zajišťující bezpečnost bezdrátové sítě na úrovni radiové části. To znamená na úroveň přístupového bodu, za ním již bezpečnost není zajišťována a musí být realizována jinými prostředky (např. HTTPS, SSH, VPN) [3, 5].

Proces šifrování začíná tím, že WEP z nešifrovaného textu vypočítá 32 bitový cyklický redundantní součet (CRC), který zajišťuje integritu dat. Tento součet se připojí za přenášenou zprávu. Dále se vezme tajný klíč a připojí se k inicializačnímu vektoru. Kombinace inicializačního vektoru a tajného klíče se předá do generátoru pseudonáhodných čísel RC4, jehož výstupem je šifrovací klíč. Šifrovací klíč je sekvence nul a jedniček dlouhá jako původní zpráva plus kontrolní součet. Dále dojde k logickému součtu XOR mezi textem spojeným kontrolním součtem a šifrovacím klíčem a výsledek je šifrovaný text.

Pokud před šifrovaný text připojíme hodnotu inicializačního klíče a mezi tímto klíčem a zašifrovanou zprávou provedeme operaci XOR dostaneme zpět původní hodnotu. Znovu se pro ni vypočítá kontrolní součet a porovná se s přijatým součtem. Pokud součty souhlasí, zpráva je v pořádku [5].

Hlavní chybou v návrhu protokolu WEP je, že není specifikováno, jak se má generovat inicializační vektor. Inicializační vektor je 24bitová hodnota přidávaná před tajný klíč. Tato kombinace slouží k inicializaci generátoru RC4. Základním požadavkem šifry RC4

je, aby za žádných okolností nebyla znovu použita stejná inicializační hodnota. Což je také problém protokolu WEP, protože není jasně definováno, jak inicializační vektor generovat. K odeslání každého paketu je potřeba, aby generátor RC4 inicializoval jinou hodnotu a v případě použití vyšších přenosových rychlostí se vyčerpá celý 24 bitový prostor inicializačního vektoru za pár hodin. V tom okamžiku se musí znovu použít použitá hodnota inicializačního vektoru a tím se porušuje základní pravidlo RC4, zakazující opakované použití stejného klíče.

Dalším bezpečnostním problémem standardu WEP je, že používá šifrovací mechanismus se sdíleným klíčem. To znamená, že používá pro šifrování i dešifrování stejnou tajnou hodnotu (klíč). Odesílatel i příjemce musí znát hodnotu klíče. Problém je v tom, že protokol 802.11 neřeší správu tohoto klíče a jeho distribuci mezi uživateli. Každý klient bezdrátové sítě obdrží klíč, který si musí ve své konfiguraci sám nastavit. S rostoucím počtem klientů tak roste pravděpodobnost, že klíč bude neoprávněně distribuován [3, 5].

WEP definuje délku klíče 40 bitů, před těchto 40 bitů se předsazuje inicializační vektor o délce 24 bitů. Někteří výrobci uvádějí, že jejich výrobky podporují 64 bitový WEP (klíč = 40 bitů + 24 bitů IV = 64 bitů) nebo i 128 bitový WEP. Tento údaj není přesný, protože 24 bitů tohoto klíče je inicializační vektor, který se přenáší nešifrovaný. To znamená, že délka klíče je 40 nebo 104 bitů [5].

I přesto že má protokol WEP řadu zranitelných míst, která výrazně omezují jeho schopnost chránit přenášená data, představuje WEP základní zabezpečení pro bezdrátové sítě nepřenášející důležitý obsah. Základním problémem WEP protokolu je chybná implementace inicializačního vektoru a tím porušení základního požadavku RC4 – nikdy neopakovat stejný klíč.

5.2 Autentizace

Autentizace neboli řízení přístupu do sítě je realizováno jako zabránění nepovolaným osobám vstupu do bezdrátové sítě. Klientské stanice bezdrátové sítě musí zažádat o autentizaci do sítě, zatímco síť se vůči stanicím autentizovat nemusí. Z tohoto pohledu má přístupový bod privilegované postavení jako součást síťové architektury [3].

802.11 specifikuje dvě metody pro autentizaci:

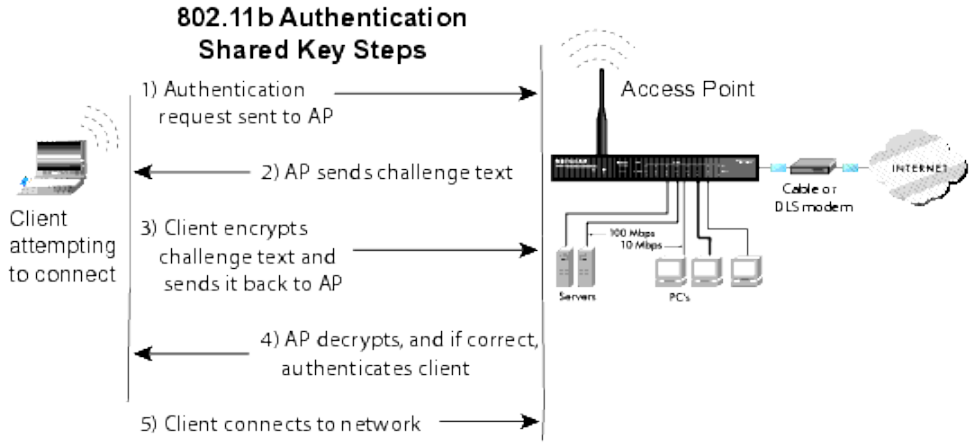
- Open-system autentizace
- Shared-key autentizace

5.2.1 Open-system autentizace

Tato metoda autentizace spočívá v tom, že přístupový bod přijme klientské zařízení na základě údajů, které mu poskytne, aniž by je ověřoval. Klient posílá svojí identifikaci v podobě SSID (Service Set Identifier). U přístupových bodů se doporučuje SSID vypnout, a to z toho důvodu, že přístupový bod, který SSID vysílá, může každá stanice přijmout a použít pro neoprávněný přístup do sítě [3].

5.2.2 Shared-key autentizace

Autentizace se sdíleným klíčem. Princip této autentizace je, že každé zařízení, které chce přistupovat do sítě, se musí prokázat přístupovým klíčem. Přístupový bod ověří platnost tohoto klíče a pak zařízení autentizuje. Ověření probíhá tak, že přístupový bod odešle náhodné číslo, bezdrátový klient toto číslo zakóduje algoritmem RC4 s pomocí přístupového klíče a odešle zpět přístupovému bodu, který je dekóduje. Pokud se dekódované číslo rovná odeslanému číslu, je klient autentizován. Standard 802.11 vyžaduje, aby každé zařízení s implementovaným WEP zabezpečením bylo schopno využívat autentizaci se sdíleným klíčem [3].



Obrázek č. 14: Autorizace Sdíleným klíčem (shared-key)

Zdroj: [18]

5.2.3 Filtrování adres

Autentizace založená na filtrování MAC adres spočívá v tom, že administrátor sítě může pro každý přístupový bod zadat seznam MAC adres, jimž je povolen přístup do bezdrátové sítě. MAC adresa je unikátní adresa každého síťového zařízení a slouží k jeho jednoznačné identifikaci.

Existují i varianty založené na autentizaci pomocí MAC adres. Například lze vytvořit seznam MAC adres, kterým je naopak přístup do sítě zakázán, omezit přístup časově anebo umožnit používat jen určitou šířku pásma atp.

Problém autentizace pomocí filtrace MAC adres je, že MAC adresa je jako jednoznačný identifikátor uložen v programovatelné paměti, lze ji tudíž měnit a tím obejít filtrování. Z tohoto důvodu se také více prosazuje používání seznamů MAC adres, které mají přístup do sítě povolen než naopak. Je obtížnější pro případné útočníky zjistit MAC adresu, která má přístup do sítě povolen než si náhodně upravit MAC adresu, která má přístup do sítě zakázán [3].

5.2.4 802.1X, EAP (Extensible Authentication Protocol) [5]

802.1X je založen na protokolu EAP, jedná se o mechanizmus přenosu EAP paketů prostřednictvím spojové vrstvy LAN. Zprávy EAP se zapouzdřují do rámců 802.1X.

Jeho základní tři komponenty jsou:

- Žadatel – klient požadující přístup k síti
- Autentizátor – typicky přístupový bod povolující nebo blokující provoz
- Autentizační server – systém udržující autentizační informace

Aby mohl řádně protokol fungovat, je nutné, aby byl jak protokol 802.1X tak zvolený EAP konzistentně podporován ve všech komponentách.

Autentizátor funguje stejně jako dynamický firewall. Dokud neproběhne autentizace, nepropustí žádný provoz kromě zpráv protokolu 802.1X. Zavádí dva virtuální porty řízený a neřízený port. Neřízený port je zpočátku v neautorizovaném stavu (je blokován veškerý provoz) po autentizaci klienta dojde k přepnutí do autentizovaného stavu a může jím procházet síťový provoz.

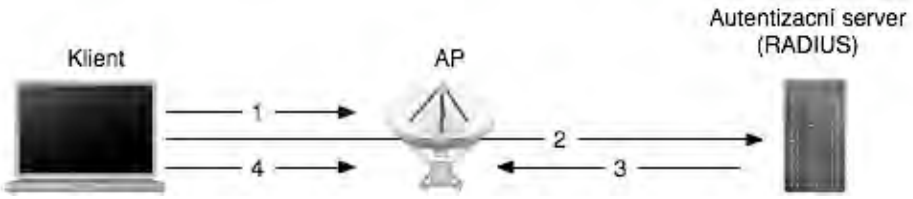
Klient (Žadatel) odešle počáteční zprávu EAP Start na přístupový bod (Autentizátor), který odpoví dotazem na identifikaci rámcem EAP Requtest/Identity.

Klient odpoví rovněž rámcem EAP Requtest/Identity, ve kterém se identifikuje. Autentizátor tuto informaci předá autentizačnímu serveru.

Autentizační server pošle přístupovému bodu zprávu obsahující povolení/zákaz přístupu daného klienta do sítě, která v sobě obsahuje informaci EAP Success/Failure a je přeposlána klientovi.

Následně provede autentizační server ověření a odpoví přístupovému bodu rámcem EAP Success/Failure. V případě obdržení rámce EAP success, přepne přístupový bod řízený

port u neautorizovaného stavu do autorizovaného stavu a povolí normální síťovou komunikaci.



Obrázek č. 15: Autentizace podle 802.1X

Zdroj: vlastní

Protokol 802.1X používá k šifrování datové komunikace pro každé autentizované zařízení dynamicky generované klíče. Tyto klíče jsou známy jen danému zařízení. Mají omezenou životnost a využívají se k šifrování rámců na daném portu, dokud se zařízení neodhlásí nebo neodpojí [3, 5].

5.3 WPA (WiFi Protected Access)

WPA je nový bezpečnostní mechanismus ratifikovaný WiFi Aliancí. Původně byl WPA vyvíjen jako bezpečnostní norma 802.11i. Bylo nutné však co nejdříve vydat nový bezpečnostní protokol a tak došlo k tomu, že se vzalo to, co už bylo hotovo v normě 802.11i a vznikl WPA, který je v podstatě podmnožinou normy 802.11i. WPA lze implementovat prostřednictvím aktualizace firmwaru a softwaru. Obsahuje nástroje šifrování TKIP (Temporal Key Integrity Protocol) a řízení přístupu (802.1X).

TKIP využívá stejného algoritmu šifrování jako WEP, používá standardně 128 bitový klíč a dočasně dynamické klíče, které pomocí automatického mechanizmu mění každých 10 000 paketů. Dále TKIP obsahuje vylepšenou funkci kontroly integrity MIC (Massage Integrity Code) a vylepšená pravidla generování inicializačního vektoru včetně sekvenčních pravidel [5]. WPA představuje řešení všech známých problémů protokolu WEP.

5.4 IEEE 802.11i

S hlavními přednostmi nové bezpečnostní normy IEEE 802.11i jsme se seznámili v přehledu doplňkových norem standardu 802.11.

AES (Advanced Encryption Standard) nabízí různé režimy činností, ve specifikaci 802.11i používá čítačový režim s protokolem CBM-MAC (Cipher Block Chaining-Message Authentication Code) obvykle označovaný jako AES-CCMP (AES-Counter Mode CBC-

MAC Protocol), který zajišťuje šifrování. CBC-MAC pak zajišťuje autentizaci a integritu dat [5].

AES šifra pracuje se symetrickým klíčem, což znamená, že text šifruje i dešifruje stejným sdíleným tajným klíčem, ale na rozdíl od šifry RC4 pracuje s bloky o velikosti 128 bitů a bývá tak označována jako bloková šifra. Celý vstupní text se rozdělí na 128 bitové bloky. Ty se postupně XORují se 128 bitovým pokaždé nově generovaným výstupem AES tak dlouho, dokud není celá zpráva zašifrována. Nakonec se čítač vynuluje a XORuje se hodnota MIC, která se přidává na konec rámce [5].

CCPM obsahuje algoritmus MIC, zajišťující ověření, že nedošlo k modifikaci přenášených dat. Výpočet MIC je založen na hlavičkových hodnotách vycházející z inicializačního vektoru a z dalších hlavičkových informací v 128bitových blocích a počítá se přes jednotlivé bloky až na konec zprávy, kde se vypočte konečná hodnota.

Výsledkem je mnohem silnější šifra, která má však zvýšené nároky na výkon. Z tohoto důvodu vyžaduje AES nový hardware a není tudíž zpětně kompatibilní s první generací bezdrátových zařízení [5].

6 Návrh a implementace v rámci zvolené sítě

6.1 Důvody, cíle a přínosy zavedení bezdrátové sítě na ISP

Pro to, aby mohl být spuštěn nějaký projekt, je třeba mít přesně stanovené cíle a důvody, proč takový projekt vůbec začínat. Některé výhody zavedení bezdrátové sítě na ISP jsou velmi významné a to zejména v konkrétním využití v akademickém prostředí. V případě zavedení WiFi na ISP by se nejednalo ani o veřejně přístupnou síť, jejímž příkladem může být například kavárna či prostor letištní haly, ani o interní, zcela uzavřenou lokální síť, dostupnou pouze pro registrované zaměstnance, jak je tomu v případě různých obchodních subjektů. Výsledkem může být několik variant různě zohledňujících, kdo se do sítě přihlašuje. Taková varianta je potom závislá především na plánovaném účelu využití a na samotné technické realizaci bezdrátové sítě [6].

Následuje přehled hlavních důvodů, proč je bezdrátová sít' na ISP zavedena. Samozřejmě jsou tyto důvody také největšími přínosy pro celou školu. Jsou rozděleny podle jednotlivých skupin uživatelů:

a) Studenti

Studenti vlastnící notebook, PDA nebo jiná mobilní zařízení již nemusí čekat na volné místo u pevných PC.

Mohou se připojit k Internetu, kdykoliv a kdekoliv (na určených místech předpokládá se poměrně husté pokrytí).

Vzniká možnost připojení takových prostor, u kterých je připojení pevnou linkou bud' příliš nákladné, nebo z jiných důvodů.

Jednoduché a ikvalitní připojení v knihovně umožní studentům připravovat se s neomezeným přístupem k informacím v klidu a na adekvátním místě.

Rozšiřují se možnosti zavedených výukových systémů. Mohou vzniknout nové kurzy s využitím bezdrátové technologie. Studenti mohou zpracovávat zadaný úkol na libovolných místech a online konzultovat s vedoucím kurzu. Také budou moci využívat své notebooky i na nepočítačových předmětech.

Sdílení znalostí s ostatními studenty bude přínosem pro větší informovanost studentů a umožní zrychlení jejich doby reakce na jakékoliv podněty.

Z dlouhodobého hlediska zavedení znamená zlepšení nejen jejich informatických znalostí, ale i zvýšení jejich všeobecné úrovně vzdělání díky rychlejšímu a kvalitnímu přístupu k informacím.

b) Učitelé

Zvýšení flexibility a mobility zaměstnanců.

Také se otvírají nové cesty ve výuce. Učitelé mají možnost vytvářet nové způsoby výuky studentů, například ideální je použití pro projektový styl práce na hodinách. Zaměstnanci mohou mít speciální přípravy na svých noteboocích a mohou je z nich prezentovat studentům přímo.

Urychlí se komunikace nejen se studenty, ale i s ostatními spolupracovníky v celém areálu školy. Možnost pracovat společně v libovolném týmu kdekoliv, např. v zasedací místnosti a sdílet dokumenty a jiné zdroje na základě vytvořeného spojení peer-to-peer.

c) Ostatní

Ideální využití pro zvané přednášky, kdy si speciální uživatelé či hosté přinesou vlastní notebook a mohou využívat přístupu k Internetu.

Obrovská výhoda pro školu jako celek je možnost využití při pořádání jakýchkoliv konferencí.

Dojde ke zvýšení prestiže školy.

d) Obecné přínosy

Především zvýšená flexibilita a mobilita uživatelů - konkrétní přínosy jsou již zmíněny výše. Jedná se o poměrně snadnou instalaci, především s využitím PoE (Power over Ethemet) dojde k výraznému zvýšení stability a kontroly nad systémem. Jednoduchá je i případná rekonfigurace sítě.

Při plánování návrh WiFi sítě je vhodné postupovat v krocích a před samotnou realizací je nutné si ujasnit některé základní aspekty budoucí bezdrátové sítě.

Propustnost sítě – požadavky na propustnost sítě patří mezi základní. Pokud chceme využít maximální propustnost, nabízí se možnost využít zařízení podporující nejnovější normu 802.11n. Pokud plánujeme provozovat na WiFi síti i zařízení založená na starších normách je vhodné zvážit, zda se vůbec vyplatí investovat do zařízení podporující novou normu.

Oblast pokrytí – požadavky na pokrytí jsou důležité při plánování větších WiFi sítí. Musíme si navrhnout orientační mapu a do ní zakreslit rozmístění přístupových bodů, antén a oblast jejich pokrytí.

Mobilita – u WiFi sítí, kde je požadována mobilita je nutné zajistit plynulé přechody od jednoho přístupového bodu ke druhému za běhu síťového připojení.

Uživatelé – počet uživatelů a jejich nároky na používání sítě je důležitý parametr v případě sdílení širokopásmového internetu. Především pak nároky uživatelů na rychlost, odezvu a

agregaci sdíleného internetu. Je důležité kapacitu sdílené internetové linky nastavit tak, aby nebyla přetěžována a byla tak zajištěna dostatečná kvalita této služby.

Logika síťového plánování – musíme navrhnout hierarchii přidělování IP adres uživatelům. Je velmi vhodné adresy přidělovat podle nějakého klíče (např. podle lokalit). Nastavit směrování provozu a rozhodnout, zda bude vhodné používat DHCP server.

Aplikace – některé specifické aplikace vyžadují pro svoji č innost podporu některých služeb přístupových bodů a ne všechna zařízení tyto služby podporují. Je tedy nutné si zjistit, jaké aplikace budou používány na dané WiFi síti a při pořizování hardwaru s tím počítat.

Bezpečnost – Nastavení síly zabezpečení sítě, především pak autentizace. Musíme se rozhodnout, zda síť bude otevřená s volným přístupem nebo s omezeným přístupem k důležitým prostředkům.

Vliv prostředí – musíme posoudit vliv prostředí na bezdrátovou síť, zjistit zda signál musí procházet přes překážky nebo jsou-li přístupové body v přímé viditelnosti atp. Zjistit ostatní sítě v dané lokalitě, vyhnout se vzájemnému rušení s ostatními bezdrátovými sítěmi.

6.2 Obecné informace

Síť je vhodné realizovat dle standardu IEEE 802.11g (WiFi). Bezdrátové síťové prvky tohoto standardu pracují v bezlicenčním pásmu 2,4 GHz a maximální dosahovaná přenosová rychlost je 54 Mbit/s. Maximální reálná přenosová rychlost je zhruba poloviční. Druhá polovina je použita pro přenos zabezpečení a ř ízení sítě. Navrhované přístupové body dokážou pracovat i dle standardu IEEE 802.11b, kdy je maximální přenosová rychlost 11 Mbit, reálně 5,5 Mbit/s. Pokud je ovšem přístupový bod v kombinovaném režimu, kdy komunikuje jak dle standardu g i b současně, nedosahuje reálně vyšších přenosových rychlostí jak 16 Mbit/s [4].

Použitá síťová zařízení

Přístupový bod:

- Cisco Aironet 1240AG Series 802.11A/B/G

Doporučená koncová zařízení:

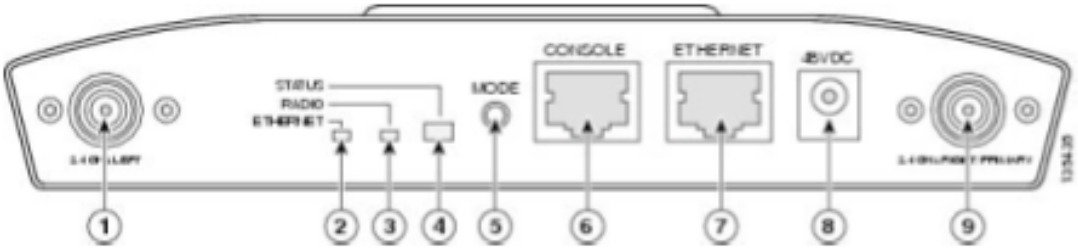
- AirPort Extreme (Wi-Fi 802.11g)
- AirPort Extreme Wi-Fi (založeno na IEEE 802.11n); IEEE 802.11a/b/g kompatibilní

6.2.1 Specifikace Cisco Aironet 1240AG Series 802.11A/B/G

Přenosové rychlosti	802.11a: 6, 9, 12, 18, 24, 36, 48, a 54 Mbps 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, a 54 Mbps
Standardy	IEEE 802.11a, 802.11b, a 802.11g
Uplink	Autosensing 802.3 10/100BASE-T Ethernet
Frekvenční pásma	2.412 to 2.472 GHz; 13 kanálů 5.15 to 5.35 GHz; 8 kanálů 5470 to 5725 MHz; 11 kanálů
Možnost připojení antén	2.4 GHz - Dual RP-TNC konektory 5 GHz – Dual RP-TNC konektory
Rozměry	16.76 x 21.59 x 2.79 cm
Váha	0,907 kg
Pracovní podmínky	Skladovací teplota: -40 to 85°C Provozní teplota: –20 to 55°C Operační vlhkost: 10 to 90 %
Paměť	32 MB RAM 16 MB flash
Příkon	100 to 240 VAC; 50 to 60Hz (zdroj) 36 to 57 VDC (zařízení)
Další možnosti napájení	Místní síť Cisco Aironet power injector 802.3 AF switche

Tabulka č. 2: Specifikace Cisco Aironet 1240

Zdroj: [19]



Obrázek č. 16: Cisco Aironet 1240

Zdroj: [19]

1. konektor 2,4 GHz antény (levý)	6. Port konzole
2. Ethernet status LED	7. port Ethernet
3. Radio status LED	8. napájecí port
4. Status LED	9. konektor 2,4 GHz antény (pravý/primární)
5. tlačítko přepínání režimu	

Tabulka č. 3: Popis jednotlivých konektorů a diod na přístupovém bodu Cisco Airone 1240

Zdroj: [19]

Obrázek č. 17: Cisco Aironet 1240

Zdroj: [19]

1. konektor 5 GHz antény (levý)	3. otvor pro bezpečnostní zámek
2. konektor 5 GHz antény (pravý/primární)	

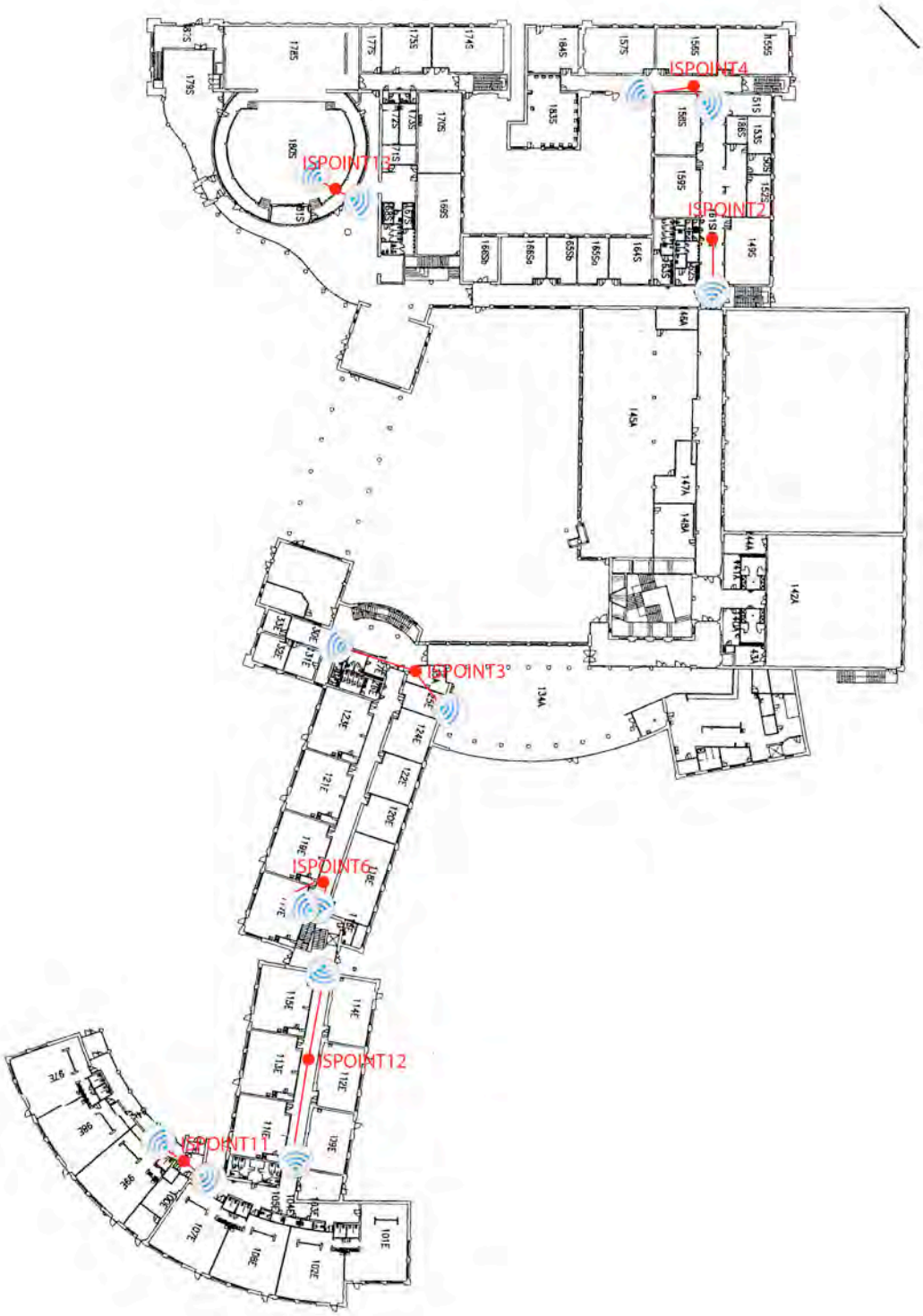
Tabulka č. 4: Popis jednotlivých konektorů a diod na přístupovém bodu Cisco Airone 1240

Zdroj: [19]

Výhodou tohoto přístupového bodu je, že k němu můžeme připojit dvojici antén. A to buď antény pracující v režimu 2,4 GHz, nebo 5 GHz. V našem případě jsem použil dvojici sektorových antén pracujících na frekvenci 2,4 GHz.

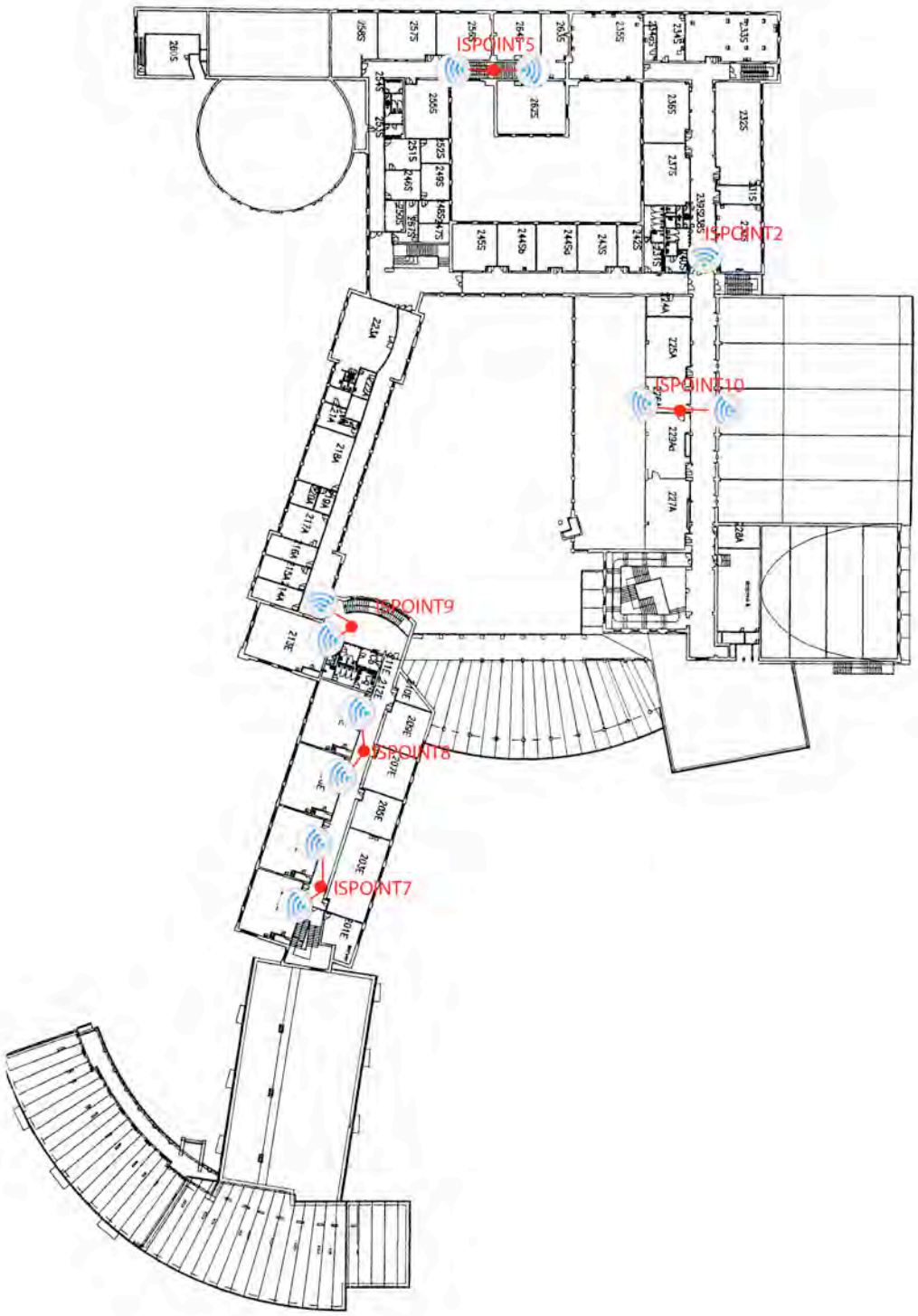
6.3 Návrh rozmístění bezdrátových přípojných bodů

Na plánech není zakreslen venkovní přístupový bod, ke kterému je připojena všesměrová anténa umístěná na komíně. Která pokrývá venkovní plochy, jako jsou parkoviště, fotbalové hřiště, tenisové a basketbalové kurty a místo s hřištěm ve školce.



Obrázek č. 18: První nadzemní patro kde se nachází školka, první stupen základní školy a druhý stupeň základní školy

Zdroj: vlastní



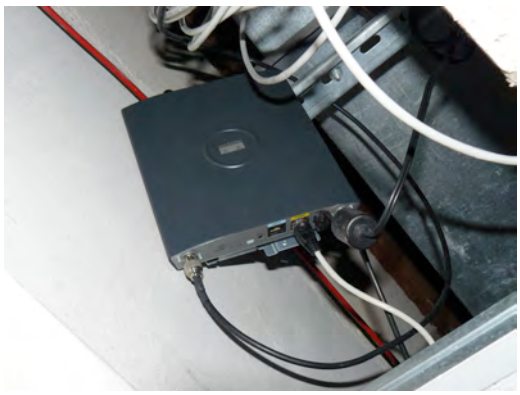
Obrázek č. 19: Druhé nadzemní patro kde se nachází nižší stupeň základní školy, střední škola, počítačové laboratoře a kanceláře

Zdroj: vlastní

Jediná část školy kde není plánováno umístit přípojný bod je tělocvična školy. Nepředpokládá se, že si studenti budou nosit počítače do výuky. V příloze č. 2 naleztnete kompletní seznam a umístění bezdrátových bodů na Mezinárodní škole. Je zde také uvedeno na jakých frekvencích mohou tyto body vysílat.

6.3.1 Instalace bezdrátového přípojného bodu

Všechny bezdrátové přípojné body jsou umístěny v podhledech na chodbách. Díky umístění v podhledech jsou skryty před zvídavými studenty a nemůže se stát, aby někdo odpojoval antény nebo je například odpojil od elektrické sítě. Tato fyzická bezpečnost je velmi důležitá, obzvláště když na tom závisí výuka. Ke každému bodu jsou připojeny dvě sektorové antény pracující na frekvencích 2,4 GHz.



Obrázek č. 20: Umístění bezdrátového bodu v pohledu

Zdroj: Vlastní

Obrázek č. 21: Umístění antény

Zdroj: Vlastní

6.4 Konfigurace bezdrátového přípojného bodu

Pro praktickou ukázku konfigurace jsem vybral jeden z přístupových bodů Cisco Aironet 1240. Tyto přístupové body patří mezi nejlépe vybavené na trhu, obsahují všechny

standardní funkce většiny současných přístupových bodů a nabízí i řadu funkcí, které nejsou standardem. Přístupový bod se konfiguruje přes webové rozhraní.

6.4.1 Základní nastavení

Přístupový bod je dodáván se zakázaným vysíláním SSID a nemá nastavenu defaultní IP adresu. Toto musíme povolit při první konfiguraci bezdrátového přístupového bodu. Přístupový bod je nastaven tak aby obdržel IP adresu z DHCP serveru. Pokud nemáme v síti DHCP server spuštěn musíme propojit bezdrátový bod s počítačem a IP adresu nakonfigurovat přes konzoli.

Nastavení	**Výchozí**
Login	Cisco (rozlišování písmen)
Heslo	Cisco (rozlišování písmen)
IP Adresa	Přidělena DHCP serverem
SSID	Nevysílá
Stav LED	**Význam**
Modrá	Normální, alespoň jeden klient je připojen
Světle zelená	Normální, není připojen žádný klient
Žlutá nebo červená	Error

Tabulka č. 4: Standardní nastavení přípojného bodu po zapnutí

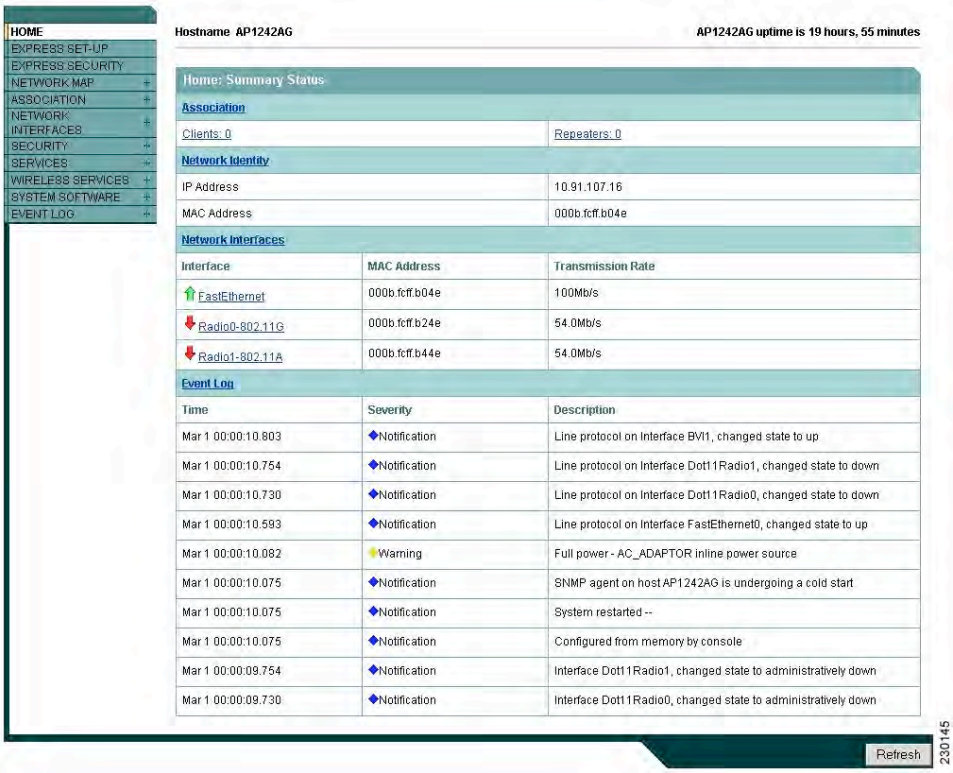
Zdroj: [19]

My na Mezinárodní škole v Praze DHCP server používáme. Toto mi velmi usnadnilo práci při vlastní konfiguraci. MAC adresa přípojného bodu je uvedena na štítku, stačilo tedy jen na DHCP serveru najít jakou IP adresu přístupový bod má. Před vlastní konfigurací bezdrátového bodu si musíme rozmyslet SSID bodu a IP adresu. A pokud budeme používat některou z metod zabezpečení tak se musím rozhodnout kterou.

Celkem je po Mezinárodní škole rozmístěno 13 přístupových bodů. Pro ukázku jsem si vybral konfiguraci jednoho z nich. Jak bylo zmíněno výše, musíme mít rozmyšleno pojmenování a IP adresy pro jednotlivé bezdrátové přípojné body. Pro pojmenování vždy bude sloužit označení ISPOINTX kde X prezentuje číslo bezdrátového přístupového bodu.

IP adresy v metalické síti jsou ze skupiny A. Pro bezdrátovou síť je určen blok adres ze skupiny B. Konkrétně pro bezdrátové přípojné body jsou to adresy 172.16.0.X kde X je číslo bezdrátového přípojného bodu.

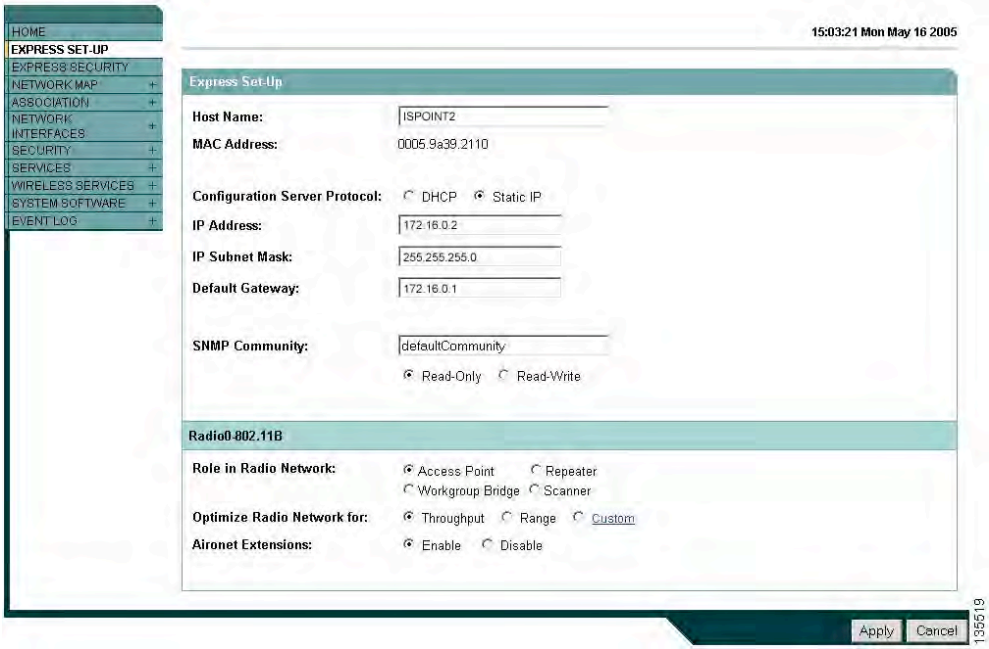
Po zadání IP adresy bezdrátového přípojného bodu do internetového prohlížeče a přihlášení vidíme následující. Levá část je vyhrazena panelu nabídek. Zde můžeme v jednotlivých sekcích konfigurovat přístupový bod. Na obrázku č. 22 je úvodní stránka bezdrátového přípojného bodu. Zde vidíme kolik je připojeno klientů, které síťové rozhraní je aktivní a záznamy chyb.



Obrázek č. 22: Úvodní stránka přístupového dobu po zadání IP adresy v prohlížeči

Zdroj: vlastní

Pro nastavení IP adresy a základních údajů slouží nabídka EXPRESS SET-UP. Která je na obrázku č. 23.



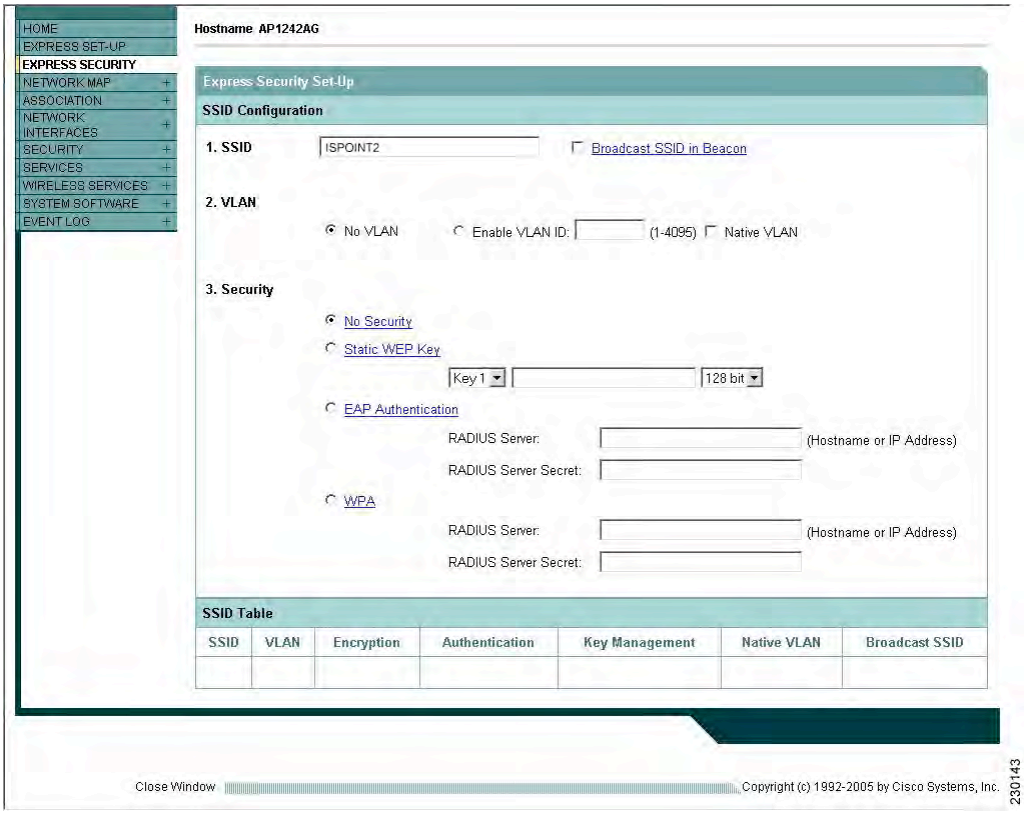
Obrázek č. 23: Express Set-Up

Zdroj: vlastní

Pokud bezdrátový bod získal adresu z DHCP serveru, musíme podle MAC adresy bodu najít na DHCP serveru jakou IP adresu má abychom ho mohli dále konfigurovat.

V Express Set-up nastavíme jméno bezdrátového bodu, jeho IP adresu, masku podsítě a defaultní bránu. Dále nastavujeme, jakou roli má tento přístupový bod v síti. Bezdrátové body mají roli Access Point. Radiovou síť optimalizujeme na výkon a povolíme rozšíření Aironet. Zmáčkneme na tlačítko Apply a naše nastavení se uloží. Pokud jsme změnili IP adresu z DHCP na statickou, musíme novou adresu zadat do prohlížeče, abychom mohli dále bezdrátový bod konfigurovat.

V panelu Express Security nastavíme, zda má bezdrátový bod vysílat SSID a také jaké. Nastavil jsem vysílání SSID stejné jako jméno bezdrátového bodu. Je to hlavně kvůli snazší identifikaci bodu v síti. Nastavení Express Security můžeme vidět na obrázku č. 24.



Obrázek č. 24: Express Security

Zdroj: vlastní

V záložce Security změníme ještě přístupové jméno a heslo pro administrátora. Ostatní nastavení necháme defaultní.

6.5 Nastavení klientů

Bezdrátové síťové adaptéry se z pohledu OS příliš neliší od klasických síťových adaptérů. Operační systém nevyžaduje žádné zvláštní prostředky k instalaci bezdrátových klientů. Většinou si vystačí s protokolem TCP/IP, který je dostupný na každém moderním OS.

V síti se vyskytují klienti s dvěma verzemi operačního systému. Jsou to počítače firmy Apple modely iBook a MacBook.

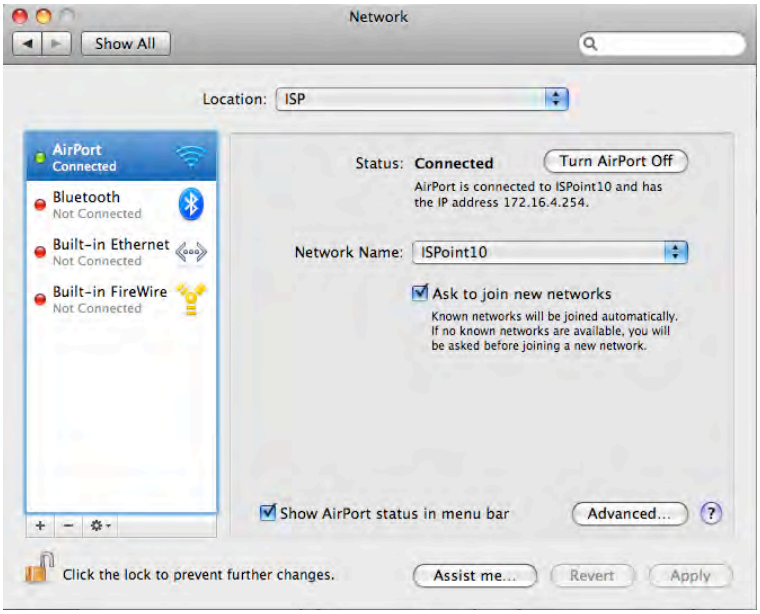
Obrázek č. 25: Apple iBook, Apple MacBook

Zdroj: [25]

Obrázek č. 26:Apple MacBook

Zdroj: [26]

Na iBoocích je operační systém Mac OS X verze 10.4 Tiger a na MacBoocích je systém Mac OS X verze 10.5 Leopard. Nastavení klientů je v podstatě stejné, proto jsem si pro ukázku vybral klienta s verzí 10.5. Na obrázku č. 27 vidíme informace o daném připojení. Vidíme, že klient je připojen, přes jaký přípojný bod se do bezdrátové sítě připojuje a jakou má IP adresu.



Obrázek č. 27: Konfigurace klienta

Zdroj: vlastní

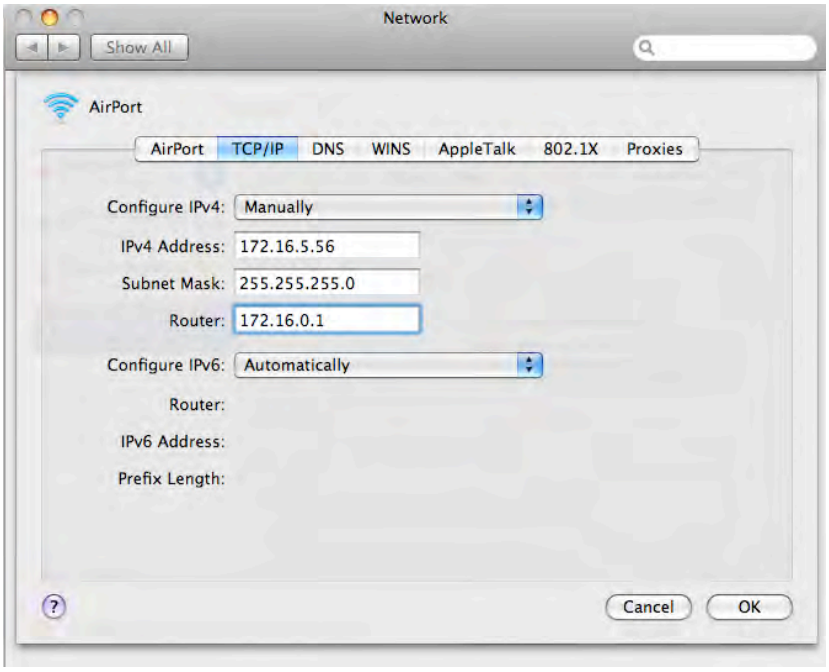
Všichni klienti v bezdrátové síti mají pevně nastavenou IP adresu. Ve školní bezdrátové síti je několik skupin uživatelů. Je to hlavne z hlediska zabezpečení sítě o kterém bude pojednáno níže. Přehled skupin uživatelů a jejich nastavení vidíte v následující tabulce.

Skupina	**IP adresy**
Studenti prvního stupně základní školy	172.16.3.1 – 172.16.3.255
Studenti druhého ročníků základní školy	172.16.2.1 – 172.16.2.255
Studenti střední školy	172.16.1.1 – 172.16.1.255
Návštěvy	172.16.4.1 – 172.16.4.255
Učitelé	172.16.5.1 – 172.16.7.255

Tabulka č. 5: Přehled bloků IP adres používaných v bezdrátové síti

Zdroj: vlastní

IP adresy pro návštěvníky školy nejsou do jejich osobních počítačů zadávány. Na školním firewallu je tento blok adres vyhrazen právě pro tyto účely a firewall je nakonfigurován pro jejich přiřazování. Na obrázku 28 můžete vidět konfiguraci klienta. Zadáváme pouze IP adresu, masku podsítě a router.



Obrázek č. 28: Konfigurace klienta

Zdroj: vlastní

6.6 Konfigurace síťové tiskárny

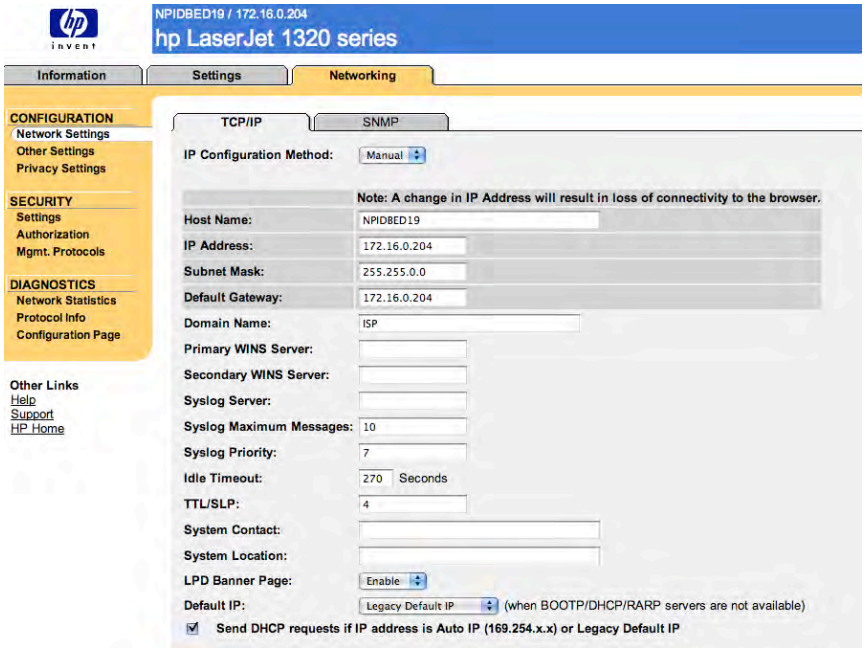
Pro potřeby studentů jsou nainstalovany ve škole celkem 4 tiskárny určené pro tisk na bezdrátové síti. Následující tabulka udává přesný typ tiskárny, její umístění a IP adresu.

Jméno	Typ	Umístění	IP adresa
MS WiFi 1	HP 2300dn	2 stupeň ZŠ	172.16.0.201
MS WiFi 2	HP 2100n	Před místností 230	172.16.0.202
US WiFi 1	HP 2100n	U schránek pro studenty SŠ	172.16.0.203
ES Gr4 & Gr5	HP 1320n	V místnosti 210	172.16.0.204

Tabulka č. 6: Přehled bezdrátových síťových tiskáren

Zdroj: vlastní

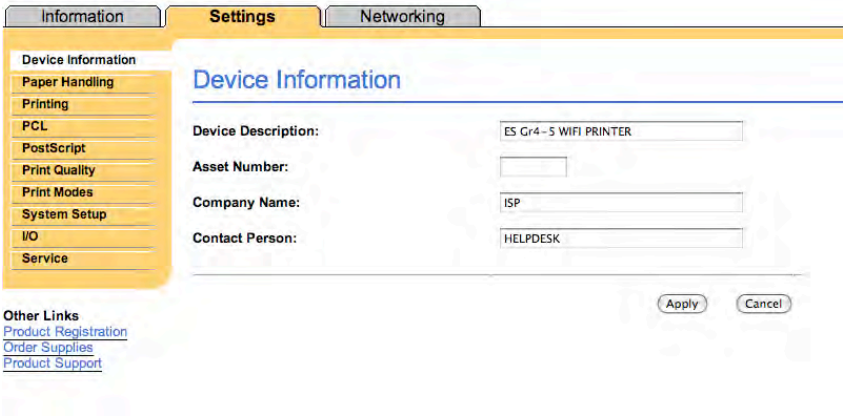
Tiskárny jsou vždy umístěny na snadno dostupných místech pro studenty. Většinou je to na místech kde se studenti pohybují nejčastěji (chodby, místnosti kde mají schránky na poštu nebo místnost kde jsou mobilní učebny po dobu dobíjení notebooků). Pro ukázku konfigurace tiskárny jsem si vybral novější model od firmy HP tiskárnu HP LaserJet 1320n. Je to moderní laserová tiskárna vybavená síťovou kartou. Pro potřeby studentů jsou tyto malé tiskárny dostačující. Tiskárna se konfiguruje přes webový prohlížeč. Z výroby je nastavena tak aby IP adresu obdržela z DHCP serveru. Na DHCP serveru si zjistíme IP adresu a zadáme ji do prohlížeče. V záložce Networking a dále Network settings nastavíme IP adresu, masku sítě a defaultní bránu.



Obrázek č. 29: Nastavení IP adresy tiskárny

Zdroj: vlastní

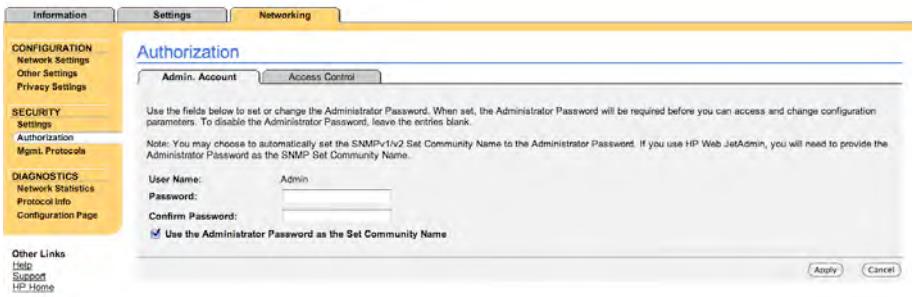
V záložce Settings a Device Information zadáme informace o tiskárně. Zadávat je nemusíme.



Obrázek č. 30: Nastavení jména

Zdroj: vlastní

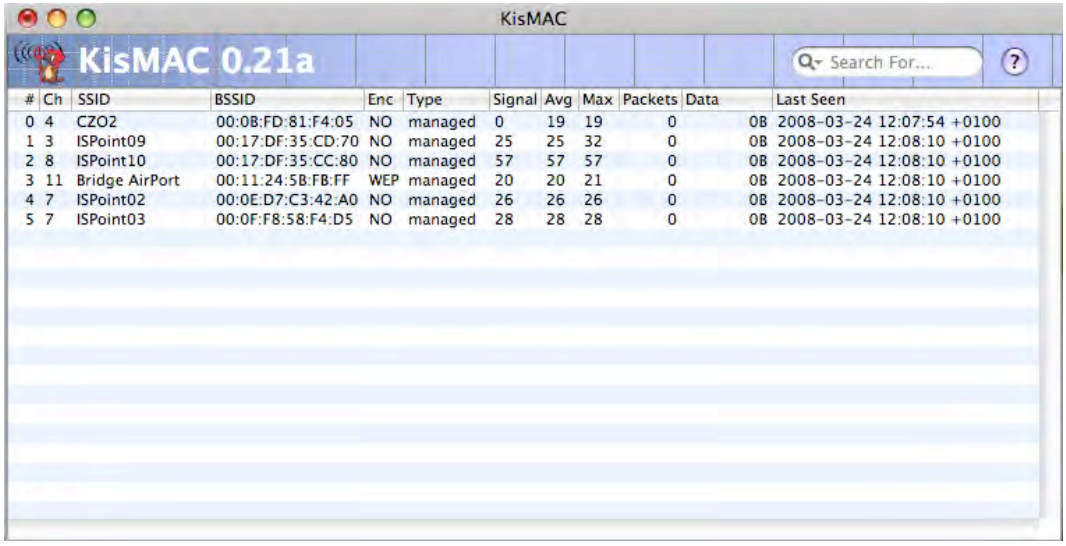
Poslední věc, kterou musím udělat je nastavení administrátorského hesla. Nastavovat ho nemusíme, ale pokud nechceme, aby nepovolaní uživatelé upravovali nastavení tiskárny, musíme toto heslo nastavit. To se provádí v záložce Networking a Authorization.



Obrázek č. 31: Změna administrátorského hesla
Zdroj: vlastní

6.7 Měření dostupnosti signálu

Měření probíhalo na počítači, se kterým studenti denně pracují. Měřit se musí se zařízením, které studenti používají proto, aby nedošlo k chybám. Každý model bezdrátové karty v běžných počítačích je od jiné firmy. Firma Apple do všech svých modelů dodává stejný typ karty AirPort Extreme. Tato karta je certifikována pro práci v sítích standardu 802.11b a 802.11g. Novější typ karty v modelech MacBook může pracovat i v sítích standardu 802.11n. Program, který jsem pro měření používal, se jmenuje KisMAC. Vychází z populárního programu netstumbler, ale je určen pro počítače Apple. Ukázku jak takové měření probíhalo, můžete vidět na obrázku.



Obrázek č. 32: Okno programu KisMAC při měření

Zdroj: vlastní

Signál byl proměřen ve všech částech školy. Měřil jsem ve všech učebnách školy, na chodbách a na všech místech kde se pohybují studenti a učitelé. Tabulky měření naleznete v příloze č. 1 této práce.

6.8 Testování v rámci mobilní učebny

Pro účely školy je mobilní učebna ideální. Jedná se o pojízdný box, vybavený notebooky včetně příslušenství (napájecí adaptéry, napájení). V současné době je na Mezinárodní škole pět takových mobilních učeben.

6.8.1 Hardwarové vybavení mobilní učebny

21 x notebook Apple iBook

parametry notebooků:

procesor	1,25 GHz PPC G4
operační paměť	512 MB
HDD	40 GB
Wifi	Apple Airport

Tabulka č. 7: Vlastnosti notebooku

Zdroj: vlastní

Dvě mobilní učebny používá první stupeň základní školy. Dvě učebny druhý stupeň základní školy a jedna mobilní učebna je pro střední školu.

Obrázek č. 33: Mobilní učebna

Zdroj: vlastní

6.8.2 Softwarové vybavení mobilní učebny

- Microsoft Office for Mac 2004
- Apple iWork08 (Pages, Keynote, Numbers) – alternativa k Microsoft Office
- iLife 06 – produkt od firmy Apple využívají se především iMovie, GarageBand a iDVD pro tvorbu multimédií
    - iMovie – střihání filmů
    - iDVD – tvroba menu k filmům
    - GarageBand – tvorba podcastů
- Inspiration8 – program pro tvorbu myšlenkových map
- Adobe Photoshop Elements – odlehčená verze Adobe Photoshop, pro jednoduchou editaci obrázků
- Adobe Illustrator – program pro práci s vektorovou grafikou
- Macromedia Dreamweaver 2004 – program pro tvorbu webových stránek
- Macromedia Flash 2004 – program pro tvorbu flash animací
- Graphical Analysis 3 – program pro tvorbu, analýzu a tisk grafů
- The Geometer's Sketchpad – matematický vizualizační software

6.8.3 Mobilní počítačová učebna

Teorie mobilní počítačové učebny

Většina škol si pořizuje učebnu přenosných počítačů právě pro jejich mobilitu. Didaktika informatiky hovoří o třech typech požadavků, které by počítačová učebna měla splňovat:

- pedagogické požadavky
- didaktické požadavky
- psychologické požadavky

Tyto požadavky by měly být brány v potaz při plánování konkrétních způsobů využívání prostředků ICT [11].

Mobilní učebna v praxi

V pěti mobilních učebnách je celkem 105 počítačů. Všichni vyučující jsou také vybaveni notebooky. Laptopy firmy Apple jsou známy pro svoji vysokou spolehlivost baterií. I při denním nabíjecím cyklu není pro notebooky problém vydržet plné zatížení i 2,5 hodiny.

V praxi to vypadá tak že pokud vyučující chce používat notebooky ve výuce, musí si je nejdříve zablokovat v rezervačním systému. Vybere si, které notebooky chce využívat, kdy a jejich počet. Ostatní učitelé tak mají přehled, kolik notebooků je ještě možné využívat ve

výuce. Žáci notebooky používají denně v průměru dvě hodiny až tři hodiny. Pokud se baterie v noteboocích během dopolední výuky vybily, dobíjeli se během pauzy na oběd.

Za celou dobu testování se nevyskytl žádný problém. A to jak s notebooky, tak s bezdrátovou sítí. Jen občas docházelo ke zpomalení sítě. To se stávalo zejména v ranních hodinách, kdy se všichni uživatelé připojovali do sítě internet. Vyřešilo se to navýšením internetové linky a hlavně omezením přístupu na některé stránky, zejména na stránky se streamovaným obsahem a multimédii.

Obrázek č. 34: Mobilní učebna v praxi

Zdroj: vlastní

7 Zabezpečení sítě

Bezdrátová počítačová síť je striktně oddělena od školní sítě. Na firewallu je bezdrátová síť oddělena a zároveň je nastavena pouze odchozí komunikace. Studenti také nemohou používat tiskárny ve vnitřní školní síti. Jsou pro ně ale vyhrazeny tiskárny, na které mohou tisknout ze školních i ze svých vlastních notebooků. Bezdrátová síť není nijak chráněna heslem. V rámci zabezpečení bezdrátové sítě se používá filtrování obsahu. Tento model se osvědčil už v drátové síti, a proto je použit i zde. K filtrování obsahu slouží software SurfControl od firmy WEBSENCE.

Přístup na webové stránky můžeme buď povolit (ALLOW), úplně zakázat (DISALLOW) nebo částečné povolit (ALLOWENCE). U částečného povolení můžeme nastavit, zda bude omezení na objem přenesených dat anebo na čas. U přenesených dat můžeme omezit v řádu MB. U času můžeme některé stránky omezit v čase vyučování anebo omezit celkový čas strávený na internetu. Máme několik skupin uživatelů a podle toho je i omezujeme. Celkově je na bezdrátové síti zakázáno stahovat z peer to peer sítí. Dále jsou zakázány stránky obsahující násilí, drogy, sexuální materiály. Na bezdrátové síti jsou zakázány komunikační programy jako je ICQ nebo MSN Messenger. Zakázané jsou Proxy servery přes které je možné na stránky se zakázaným obsahem přistupovat. Studenti mají zakázána streamovaná média a hraní online her. Povolen je přístup k webovému emailu, stránkám s cestováním, různé vyhledávače a encyklopedie. Časově nebo datově omezeny jsou stránky s nakupováním, s přehráváním hudby.

Rozdělení je velmi výhodné. Někteří učitelé například ve výuce potřebují povolit určité stránky a tak dočasně dostanou oprávnění a mohou se studenty pracovat na projektech. Pro uživatele, kteří IP adresu obdrží automaticky z DHCP serveru je omezení největší. Dostanou se pouze na email a na základní stránky. Je zakázáno nakupování, streamovaná media, stahovaní. K rozdělení do skupin a nastavení pevných IP adres jsem byl nucen přistoupit, protože někteří studenti hrubě porušovali pravidla a stahovali velké objemy dat především z peer-to-peer sítí.

V následující přehledné tabulce uvádím, jaká jsou pravidla pro studenty a jaká pravidla jsou pro učitele, pokud jsou s počítači připojeni k bezdrátové síti.

Pravidla SurfControlu	**Učitelé**	**Studenti**
ISP servers	Allow	Allow
Adult/Sexual Explicit	Disallow	Disallow
ISP Allowed	Allow	Allow
Travel	Allow	Allow
Shopping	Allowance – 60 min WT	Allowance – 30 min WT
Finance&Investment	Allowance - 60 min WT	Allowance – 30 min WT
Web-based Email	Allow	Allow
Computing & Internet	Allow	Allow
Peer-to-peer	Disallow	Disallow
Games	Disallow	Disallow
ISP blocked	Disallow	Disallow
Proxies	Disallow	Disallow
Gambling, intolerance, criminal, violence, weapons, illegal drugs, tabacco, hacking	Disallow	Disallow
Executables	Disallow	Disallow
Personals&Dating	Disallow	Disallow
Chat	Allowence – 30 min WT	Allowence – 30 min WT
Messengers	Disallow	Disallow
Glamour&Intimate Apparel	Disallow	Disallow
Spyware	Disallow	Disallow
Streaming media	Allowance – 50 MB	Allowance – 50 MB
Entertainment	Allowance – 60 min WT	Allowance – 30 min WT
Sports	Allowance – 120 min WT	Allowance – 60 min WT
YouTube	Allowance – 30 MB	Disallow
Audio files	Allowance – 50 MB	Allowance – 50 MB

Tabulka č. 8: Pravidla pro filtrování

Zdroj: vlastní

8 Závěr

Bakalářskou práci jsem zpracovával pro Mezinárodní školu v Praze. Tématem mé práce bylo vytvořit návrh školní bezdrátové sítě. V obecné části bakalářské práci se zabývám obecnými principy tvorby bezdrátových sítí, především pak tvorbou sítí založených na standardu IEEE 802.11 neboli WiFi. Shrnuji zde poznatky týkající se návrhu, správy, zabezpečení a konkrétní realizací těchto sítí. Při popisu služeb, které WiFi sítě používají, se snažím poskytnout přehled současné technologie založené na WiFi sítích. Poukazuji na výhody, které WiFi sítě svým uživatelům nabízejí a nechybí ani uvedení praktických možností jak tyto služby použít formou doporučení, které vycházejí z praktických zkušeností.

Zvláštní pozornost jsem věnoval bezpečnosti WiFi sítí, což byla především zpočátku vývoje této technologie, často opomíjená kapitola. Masivní rozšíření WiFi sítí mezi širokou veřejnost v posledních letech však ukázalo, že podcenění bezpečnosti WiFi sítí má za následek odrazení většiny potencionálních firemních zákazníků. Výrobci na tuto situaci v posledních letech velmi rychle zareagovali a podařilo se jim většinu bezpečnostních děr a nedostatků odstranit. V současné době se tak WiFi sítě stali zajímavé i pro firemní zákazníky.

V závěru práce jsem uvedl praktický příklad konfigurace přístupového bodu a klientské stanice. Tyto dva aktivní prvky WiFi sítí jsou základními kameny pro výstavbu těchto sítí. Praktická ukázka konfigurace přístupového bodu aplikuje teoretické poznatky z úvodní části práce. Umožňuje tak čtenářům snadno navrhnout, vytvořit a spravovat bezdrátovou WiFi síť, což bylo také hlavním cílem této bakalářské práce.

Po bezmála ročním provozu bezdrátové sítě se nevyskytly závažnější problémy se sítí. V příštím roce zavádí škola program 1TO1 je navrženo koupit Wireless kontroler a cca 7 dalších bezdrátových bodů. Zvýší se tak dostupnost signálu a díky Wireless kontroleru i jeho distribuce.

9 Resume

9.1 Resume v češtině

Jako téma své bakalářské práce jsem si vybral Návrh bezdrátové počítačové sítě pro Mezinárodní školu v Praze. Chtěl jsem si prohloubit své znalosti o síťových technologiích a to zejména o bezdrátových sítích a jejich bezpečnosti. Při návrhu rozmístění bezdrátových bodů jsem využil znalostí z přednášek ve škole.

Za nejdůležitější část považuji nastavení zabezpečení. Škola není typická firma a tak je potřeba vytvořit spoustu pravidel pro jednotlivé skupiny studentů a zaměstnanců školy. Bylo velmi těžké rozhodnout, zda daný uživatel má na určité věci oprávnění nebo už nikoli. Další velmi důležitou částí je proměření síly signálu v jednotlivých částech školy. Toto byla časově velmi náročná práce. Škola leží na 6ha pozemku a jen samotná zastavěná plocha je 2ha.

V praxi se moje práce osvědčila a studenti a učitelé jsou velmi spokojeni s přístupem k nejmodernějším technologiím. Díky této práci bylo rozhodnuto od příštího školního roku přejít na program 1TO1.

Během řešení bakalářské práce jsem se naučil spoustu nových věcí z oboru sítí. Získal jsem mnoho zkušeností s návrhem a konfigurací a dostal jsem se k nejmodernějším technologiím.

9.2 Resume v angličtině

I have chosen „Wireless network design“ for International School of Prague as a topic of my bachelor thesis. My goal is to deepen my knowledge of network technologies, mainly wireless networks and their security. I have used my school knowledge on the network design and security.

I think that the most important part is network security. The school is not a typical company, so it is necessary to create rules for each group of students and their teachers. It was very difficult to decide whether some user has the rights yet or not. Another very important part was the signal measuring in each section of school. It was quite time-consuming because the International School is rather big.

Students and teachers are very satisfied with the current wireless solution and access to the most recent technologies. After this pilot program it was decided to proceed with the “one to one laptop program”.

Working on this thesis has provided me with a lot of experience in network administration. I have learned about network design and administration and I have become familiar with the newest technologies.

10 Použitá literatura:

[1]Microsoft press: Základy sítí. Computer Press 1999

ISBN 80-7226-158-4

[2]Brisbin S.: WiFi: Postavte si svou vlastní wi-fi síť. Neocortex, Praha 2002. ISBN 80-86330-13-3

[3]Zandl P.: Bezdrátové sítě WiFi: praktický průvodce. Computer Press, Brno 2003 ISBN 80-7226-632-2

[4]Velte Toby J., Velte Anthony T.: Síťové technologie Cisco. Computer Press, Brno 2003, ISBN 80-7226-857-0

[5]Barken L.: WiFi: jak zabezpečit bezdrátovou síť. Computer Press, Brno 2004. ISBN 80-251-0346-3

[6] Livingston P. 2006: 1-to1 Learning Laptop Programs That Work. International Society for Technology in Education

[7] Wikipedie otevřená encyklopedie [online]. [cit. 10.2.2008]. Dostupný na WWW:

http://cs.wikipedia.org/wiki/IrDA

[8] Wikipedia, the free encyklopedia [online]. [cit. 10.2.2008]. Dostupný na WWW:

http://en.wikipedia.org/wiki/Peer_to_peer

[9] Tomáš Richtr – mobilní komunikace

http://tomas.richtr.cz/mobil/hiper.htm

[10] Připojte se – novinky ze světa internetu

http://www.pripojtese.cz/art_doc577B07067CF80B82C125722800539FF3.html

[11] Metodický portál o vzdělávání

http://www.rvp.cz/clanek/2094

[12] Wi-Fi Alliance [online]. 2007, [cit. 10.2.2008]. Dostupný na WWW:

http://www.wi-fi.org/brand_usage.php

[13] Petri IT knowledgebase [online] 2007, [cit. 10..2.2008]. Dostupný na WWW: http://www.petri.co.il/osi_concepts.htm

[14] ARC Communications Research Network [online] 2004, [cit. 10.2.2008] Dostupný na WWW: http://www.acorn.net.au/report/adhocnetworks/adhocnetworks.cfm

[15] Cisco Aironet 1240 AG Series - Products & Services - Cisco Systems [online] 1992-2008, [cit. 11.2.2008]. Dostupný na WWW: http://www.cisco.com/en/US/products/ps6521

[16] D-Link Česká republik stárnky výrobce bezdrátové techniky [online] 2004-2008,

[cit. 11.2.2008]. Dostpný na WWW:
http://www.dlink.cz/?go=jN7uAYLx/oIJaWVUC7YcU9f8nJUIKOZTScSwf7LknV/gUIl3jw==
[17] Edimax Technology [online] 2007, [cit. 11.2.2008]. Dostupný na WWW: http://www.edimax.com/en/produce_detail.php?pl1_id=1&pl2_id=8&pl3_id=23&pd_id=29
[18] NETGEAR Connect with Inovation [online] 1998 – 2006, [cit. 12.2.2008]. Dostupný na WWW:
http://documentation.netgear.com/reference/fra/wireless/WirelessNetworkingBasics-3-09.htm
[19] Quick Start Guide Cisco Aironet 1240AG Series Access Point, manuál
k přístupovému bodu Cisco Aironet 1240 AG
[20] Wikipedia, the free encyclopedia [online], cit [9.2.2008]. Dostupný na WWW:
http://en.wikipedia.org/wiki/802.11
[21] Wikipedie otevřená encyklopedie [online]. [cit. 14.2.2008]. Dostupný na WWW:
http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5
[22] Communication by light [online]. [cit. 15.2.2008]. Dostupný na WWW:
http://www.cbl.cz/show.php?cat=15
[23] Wikipedie otevřená encyklopedie [online]. [cit. 14.2.2008]. Dostupný na WWW:
http://cs.wikipedia.org/wiki/MIMO
[24] Wikipedia the free enczklopedia [online]. [cit. 16.2.2008] Dostupný na WWW:
http://en.wikipedia.org/wiki/802.11n
[25] What Computer is best for digital photography [online]. [cit. 15.2.2008] Dostupný na WWW:
http://www.kenrockwell.com/apple/which-mac.htm
[26] Apple Technology web page [online]. [cit. 15.2.2008] Dostupný na WWW:
http://techpaedia.com/apple/2006/08/

11 Přílohy

Příloha č. 1 – Protokol měření síly a dostupnosti signálu

Příloha č. 2 - Přehled bezdrátových bodů a jejich umístění

Příloha č. 1 – Protokol měříní síly a dostupnosti signal

měření: chodba před 109e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint01	00:0F:F8:58:E7:72	-90	-90	7
ISPoint12	00:1C:B0:E8:31:00	-38	-69	5
ISPoint08	00:17:DF:35:E0:70	-89	-90	1
ISPoint11	00:1C:B0:E8:30:B0	-66	-90	12
ISPoint07	00:17:DF:35:E1:20	-90	-90	13

měření: chodba před 115e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint12	00:1C:B0:E8:31:00	-35	-53	5
ISPoint08	00:17:DF:35:E0:70	-57	-90	1
ISPoint11	00:1C:B0:E8:30:B0	-74	-90	12

měření: chodba před 124e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint01	00:0F:F8:58:E7:72	-62	-90	7
ISPoint06	00:17:DF:35:CE:20	-67	-90	11
ISPoint12	00:1C:B0:E8:31:00	-77	-90	5
ISPoint08	00:17:DF:35:E0:70	-54	-90	1
ISPoint07	00:17:DF:35:E1:20	-90	-90	13
ISPoint09	00:17:DF:35:CD:70	-90	-90	3
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7

měření: chodba před 148a

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint03	00:0F:F8:58:F4:D5	-68	-90	7
ISPoint10	00:17:DF:35:CC:80	-90	-90	8
ISPoint05	00:0F:F8:58:FF:FA	-70	-90	7

měření: chodba před 181s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint01	00:0F:F8:58:E7:72	-87	-90	7
ISPoint09	00:17:DF:35:CD:70	-90	-90	3
ISPoint02	00:0E:D7:C3:42:A0	-75	-90	7
ISPoint10	00:17:DF:35:CC:80	-69	-90	8
ISPoint13	00:1C:B0:E8:33:80	-47	-72	1
ISPoint06	00:17:DF:35:CE:20	-90	-90	11
ISPoint07	00:17:DF:35:E1:20	-90	-90	13

měření: chodba před 183s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint03	00:0F:F8:58:F4:D5	-90	-90	7
ISPoint05	00:0F:F8:58:FF:FA	-27	-56	7
ISPoint04	00:0F:F8:58:FF:F7	-90	-90	7

měření: chodba před 202e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint06	00:17:DF:35:CE:20	-67	-79	11
ISPoint12	00:1C:B0:E8:31:00	-68	-78	5
ISPoint08	00:17:DF:35:E0:70	-59	-68	1
ISPoint07	00:17:DF:35:E1:20	-49	-54	13
ISPoint11	00:1C:B0:E8:30:B0	-90	-90	12
ISPoint01	00:0F:F8:58:E7:72	-90	-90	7

měření: chodba před 213e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint13	00:1C:B0:E8:33:80	-90	-90	1
ISPoint01	00:0F:F8:58:E7:72	-66	-76	7
ISPoint07	00:17:DF:35:E1:20	-90	-90	13
ISPoint10	00:17:DF:35:CC:80	-84	-90	8
ISPoint06	00:17:DF:35:CE:20	-66	-86	11
ISPoint09	00:17:DF:35:CD:70	-55	-67	3
ISPoint02	00:0E:D7:C3:42:A0	-64	-90	7
ISPoint08	00:17:DF:35:E0:70	-90	-90	1

měření: chodba před 216a

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint10	00:17:DF:35:CC:80	-80	-90	8
ISPoint09	00:17:DF:35:CD:70	-30	-56	3
ISPoint02	00:0E:D7:C3:42:A0	-57	-73	7
ISPoint01	00:0F:F8:58:E7:72	-73	-90	7
ISPoint06	00:17:DF:35:CE:20	-86	-90	11

měření: chodba před 226a

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint03	00:0F:F8:58:F4:D5	-54	-90	7
ISPoint09	00:17:DF:35:CD:70	-90	-90	3
ISPoint10	00:17:DF:35:CC:80	-31	-67	8
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7

měření: chodba před 265v

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint10	00:17:DF:35:CC:80	-63	-90	8
ISPoint09	00:17:DF:35:CD:70	-89	-90	3
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint03	00:0F:F8:58:F4:D5	-69	-73	7
ISPoint01	00:0F:F8:58:E7:72	-90	-90	7

měření: jidelna

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint07	00:17:DF:35:E1:20	-90	-90	13
ISPoint10	00:17:DF:35:CC:80	-74	-90	8
ISPoint01	00:0F:F8:58:E7:72	-35	-90	7
ISPoint09	00:17:DF:35:CD:70	-72	-90	3
ISPoint02	00:0E:D7:C3:42:A0	-67	-90	7
ISPoint12	00:1C:B0:E8:31:00	-73	-90	5
ISPoint08	00:17:DF:35:E0:70	-90	-90	1
ISPoint06	00:17:DF:35:CE:20	-84	-90	11
ISPoint13	00:1C:B0:E8:33:80	-90	-90	1

měření: místnost 94e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint09	00:17:DF:35:CD:70	-86	-90	3
ISPoint12	00:1C:B0:E8:31:00	-71	-90	5
ISPoint08	00:17:DF:35:E0:70	-73	-90	1
ISPoint11	00:1C:B0:E8:30:B0	-50	-71	12
ISPoint07	00:17:DF:35:E1:20	-80	-90	13
ISPoint06	00:17:DF:35:CE:20	-90	-90	11
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint13	00:1C:B0:E8:33:80	-90	-90	1

měření: místnost 97e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint09	00:17:DF:35:CD:70	-90	-90	3
ISPoint07	00:17:DF:35:E1:20	-82	-90	13
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint13	00:1C:B0:E8:33:80	-90	-90	1
ISPoint11	00:1C:B0:E8:30:B0	-90	-90	12
ISPoint06	00:17:DF:35:CE:20	-90	-90	11
ISPoint12	00:1C:B0:E8:31:00	-90	-90	5
ISPoint08	00:17:DF:35:E0:70	-90	-90	1

měření: místnost 98e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint08	00:17:DF:35:E0:70	-87	-90	1
ISPoint11	00:1C:B0:E8:30:B0	-69	-90	12
ISPoint07	00:17:DF:35:E1:20	-90	-90	13
ISPoint12	00:1C:B0:E8:31:00	-90	-90	5

měření: místnost 99e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint11	00:1C:B0:E8:30:B0	-61	-90	12
ISPoint07	00:17:DF:35:E1:20	-90	-90	13
ISPoint12	00:1C:B0:E8:31:00	-90	-90	5
ISPoint09	00:17:DF:35:CD:70	-90	-90	3

měření: místnost 101e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint12	00:1C:B0:E8:31:00	-90	-90	5
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint11	00:1C:B0:E8:30:B0	-68	-90	12
ISPoint01	00:0F:F8:58:E7:72	-90	-90	7

měření: místnost 102e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint11	00:1C:B0:E8:30:B0	-65	-89	12
ISPoint12	00:1C:B0:E8:31:00	-90	-90	5

měření: místnost 103e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint01	00:0F:F8:58:E7:72	-90	-90	7
ISPoint11	00:1C:B0:E8:30:B0	-51	-59	12
ISPoint12	00:1C:B0:E8:31:00	-84	-90	5

měření: místnost 106e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint12	00:1C:B0:E8:31:00	-72	-90	5
ISPoint11	00:1C:B0:E8:30:B0	-54	-90	12

měření: místnost 107e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint11	00:1C:B0:E8:30:B0	-52	-69	12
ISPoint07	00:17:DF:35:E1:20	-90	-90	13
ISPoint12	00:1C:B0:E8:31:00	-90	-90	5
ISPoint08	00:17:DF:35:E0:70	-90	-90	1

měření: místnost 109e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint01	00:0F:F8:58:E7:72	-90	-90	7
ISPoint12	00:1C:B0:E8:31:00	-60	-75	5
ISPoint11	00:1C:B0:E8:30:B0	-65	-86	12
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7

měření: místnost 110e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint12	00:1C:B0:E8:31:00	-55	-82	5
ISPoint08	00:17:DF:35:E0:70	-90	-90	1
ISPoint11	00:1C:B0:E8:30:B0	-53	-72	12
ISPoint07	00:17:DF:35:E1:20	-90	-90	13

měření: místnost 112e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint01	00:0F:F8:58:E7:72	-90	-90	7
ISPoint12	00:1C:B0:E8:31:00	-51	-71	5
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint08	00:17:DF:35:E0:70	-90	-90	1
ISPoint11	00:1C:B0:E8:30:B0	-87	-90	12

měření: místnost 113e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint12	00:1C:B0:E8:31:00	-35	-65	5
ISPoint08	00:17:DF:35:E0:70	-87	-90	1
ISPoint11	00:1C:B0:E8:30:B0	-72	-90	12
ISPoint07	00:17:DF:35:E1:20	-90	-90	13
ISPoint06	00:17:DF:35:CE:20	-90	-90	11
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7

měření: místnost 114e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint01	00:0F:F8:58:E7:72	-73	-90	7
ISPoint12	00:1C:B0:E8:31:00	-45	-57	5
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint08	00:17:DF:35:E0:70	-85	-90	1
ISPoint07	00:17:DF:35:E1:20	-90	-90	13

měření: místnost 115e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint06	00:17:DF:35:CE:20	-90	-90	11
ISPoint12	00:1C:B0:E8:31:00	-39	-62	5
ISPoint08	00:17:DF:35:E0:70	-67	-89	1
ISPoint07	00:17:DF:35:E1:20	-82	-90	13
ISPoint11	00:1C:B0:E8:30:B0	-90	-90	12
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint09	00:17:DF:35:CD:70	-90	-90	3

měření: místnost 118e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint12	00:1C:B0:E8:31:00	-74	-90	5
CzF.NebuNet.GA2	00:0B:6B:57:D6:28	-76	-90	6
ISPoint08	00:17:DF:35:E0:70	-50	-72	1
ISPoint07	00:17:DF:35:E1:20	-67	-90	13
ISPoint06	00:17:DF:35:CE:20	-89	-90	11
ISPoint01	00:0F:F8:58:E7:72	-90	-90	7
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7

měření: místnost 119e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint06	00:17:DF:35:CE:20	-70	-90	11
ISPoint12	00:1C:B0:E8:31:00	-87	-90	5
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint08	00:17:DF:35:E0:70	-49	-68	1
ISPoint07	00:17:DF:35:E1:20	-68	-90	13
ISPoint09	00:17:DF:35:CD:70	-90	-90	3

měření: místnost 120e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint06	00:17:DF:35:CE:20	-70	-90	11
ISPoint08	00:17:DF:35:E0:70	-64	-90	1
ISPoint07	00:17:DF:35:E1:20	-73	-90	13
ISPoint12	00:1C:B0:E8:31:00	-90	-90	5
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint01	00:0F:F8:58:E7:72	-90	-90	7

měření: místnost 121e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint06	00:17:DF:35:CE:20	-58	-90	11
ISPoint08	00:17:DF:35:E0:70	-65	-75	1
ISPoint02	00:0E:D7:C3:42:A0	-82	-90	7
ISPoint07	00:17:DF:35:E1:20	-71	-90	13
ISPoint01	00:0F:F8:58:E7:72	-90	-90	7
ISPoint12	00:1C:B0:E8:31:00	-90	-90	5
ISPoint09	00:17:DF:35:CD:70	-90	-90	3

měření: místnost 122e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint06	00:17:DF:35:CE:20	-73	-90	11
ISPoint08	00:17:DF:35:E0:70	-68	-90	1
ISPoint07	00:17:DF:35:E1:20	-90	-90	13
ISPoint01	00:0F:F8:58:E7:72	-69	-90	7
ISPoint09	00:17:DF:35:CD:70	-90	-90	3
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7

měření: místnost 123e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint01	00:0F:F8:58:E7:72	-71	-90	7
ISPoint09	00:17:DF:35:CD:70	-74	-90	3
ISPoint06	00:17:DF:35:CE:20	-58	-74	11
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint08	00:17:DF:35:E0:70	-72	-90	1
ISPoint07	00:17:DF:35:E1:20	-90	-90	13

měření: místnost 124e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint01	00:0F:F8:58:E7:72	-59	-90	7
ISPoint06	00:17:DF:35:CE:20	-77	-90	11
ISPoint07	00:17:DF:35:E1:20	-90	-90	13
ISPoint08	00:17:DF:35:E0:70	-72	-90	1

měření: místnost 142a

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint10	00:17:DF:35:CC:80	-90	-90	8
ISPoint01	00:0F:F8:58:E7:72	-90	-90	7
ISPoint09	00:17:DF:35:CD:70	-90	-90	3
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7

měření: místnost 145a

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint10	00:17:DF:35:CC:80	-48	-85	8
ISPoint09	00:17:DF:35:CD:70	-73	-90	3
ISPoint03	00:0F:F8:58:F4:D5	-73	-90	7
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint01	00:0F:F8:58:E7:72	-71	-90	7
ISPoint06	00:17:DF:35:CE:20	-90	-90	11
ISPoint05	00:0F:F8:58:FF:FA	-90	-90	7

měření: místnost 155s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint03	00:0F:F8:58:F4:D5	-63	-90	7
ISPoint05	00:0F:F8:58:FF:FA	-40	-76	7

měření: místnost 156s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint05	00:0F:F8:58:FF:FA	-50	-66	7
ISPoint03	00:0F:F8:58:F4:D5	-60	-90	7
ISPoint04	00:0F:F8:58:FF:F7	-90	-90	7

měření: místnost 157s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint03	00:0F:F8:58:F4:D5	-90	-90	7
ISPoint05	00:0F:F8:58:FF:FA	-53	-90	7
ISPoint04	00:0F:F8:58:FF:F7	-90	-90	7

měření: místnost 158s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint03	00:0F:F8:58:F4:D5	-61	-90	7
ISPoint05	00:0F:F8:58:FF:FA	-48	-74	7
ISPoint04	00:0F:F8:58:FF:F7	-90	-90	7

měření: místnost 159s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint03	00:0F:F8:58:F4:D5	-58	-90	7
ISPoint05	00:0F:F8:58:FF:FA	-61	-87	7
ISPoint04	00:0F:F8:58:FF:F7	-90	-90	7

měření: místnost 164s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint03	00:0F:F8:58:F4:D5	-76	-90	7
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint10	00:17:DF:35:CC:80	-68	-90	8
ISPoint05	00:0F:F8:58:FF:FA	-69	-90	7
ISPoint04	00:0F:F8:58:FF:F7	-90	-90	7

měření: místnost 165sa

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint10	00:17:DF:35:CC:80	-68	-90	8
ISPoint03	00:0F:F8:58:F4:D5	-90	-90	7
ISPoint05	00:0F:F8:58:FF:FA	-67	-90	7
ISPoint04	00:0F:F8:58:FF:F7	-69	-90	7
ISPoint09	00:17:DF:35:CD:70	-90	-90	3
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint13	00:1C:B0:E8:33:80	-90	-90	1

měření: místnost 165sb

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint05	00:0F:F8:58:FF:FA	-69	-90	7
ISPoint04	00:0F:F8:58:FF:F7	-65	-90	7
ISPoint09	00:17:DF:35:CD:70	-85	-90	3
ISPoint10	00:17:DF:35:CC:80	-72	-90	8
ISPoint03	00:0F:F8:58:F4:D5	-90	-90	7
ISPoint13	00:1C:B0:E8:33:80	-90	-90	1

měření: místnost 166sa

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint10	00:17:DF:35:CC:80	-90	-90	8
ISPoint05	00:0F:F8:58:FF:FA	-68	-90	7
ISPoint04	00:0F:F8:58:FF:F7	-57	-88	7
ISPoint13	00:1C:B0:E8:33:80	-90	-90	1
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint03	00:0F:F8:58:F4:D5	-90	-90	7

měření: místnost 178s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint04	00:0F:F8:58:FF:F7	-64	-90	7
ISPoint13	00:1C:B0:E8:33:80	-66	-90	1

měření: místnost 180s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint13	00:1C:B0:E8:33:80	-60	-90	1
ISPoint04	00:0F:F8:58:FF:F7	-72	-90	7

měření: místnost 183s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint05	00:0F:F8:58:FF:FA	-47	-90	7
ISPoint04	00:0F:F8:58:FF:F7	-64	-90	7
ISPoint03	00:0F:F8:58:F4:D5	-90	-90	7

měření: místnost 184s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint05	00:0F:F8:58:FF:FA	-65	-79	7
ISPoint04	00:0F:F8:58:FF:F7	-69	-90	7

měření: místnost 202e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint06	00:17:DF:35:CE:20	-68	-90	11
ISPoint12	00:1C:B0:E8:31:00	-83	-90	5
ISPoint08	00:17:DF:35:E0:70	-50	-90	1
ISPoint07	00:17:DF:35:E1:20	-35	-63	13
ISPoint09	00:17:DF:35:CD:70	-90	-90	3
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint11	00:1C:B0:E8:30:B0	-90	-90	12

měření: místnost 203e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint01	00:0F:F8:58:E7:72	-86	-90	7
ISPoint06	00:17:DF:35:CE:20	-61	-75	11
ISPoint08	00:17:DF:35:E0:70	-67	-90	1
ISPoint07	00:17:DF:35:E1:20	-50	-67	13
ISPoint12	00:1C:B0:E8:31:00	-74	-90	5
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7

měření: místnost 204e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint06	00:17:DF:35:CE:20	-53	-77	11
ISPoint02	00:0E:D7:C3:42:A0	-87	-90	7
ISPoint08	00:17:DF:35:E0:70	-67	-90	1
ISPoint07	00:17:DF:35:E1:20	-28	-59	13
ISPoint09	00:17:DF:35:CD:70	-90	-90	3
ISPoint12	00:1C:B0:E8:31:00	-90	-90	5
ISPoint01	00:0F:F8:58:E7:72	-90	-90	7

měření: místnost 205e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint01	00:0F:F8:58:E7:72	-86	-90	7
ISPoint09	00:17:DF:35:CD:70	-90	-90	3
ISPoint12	00:1C:B0:E8:31:00	-90	-90	5
ISPoint08	00:17:DF:35:E0:70	-79	-90	1
ISPoint07	00:17:DF:35:E1:20	-57	-75	13
ISPoint06	00:17:DF:35:CE:20	-53	-67	11
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7

měření: místnost 206e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint09	00:17:DF:35:CD:70	-84	-90	3
ISPoint06	00:17:DF:35:CE:20	-30	-55	11
ISPoint02	00:0E:D7:C3:42:A0	-74	-90	7
ISPoint08	00:17:DF:35:E0:70	-90	-90	1
ISPoint07	00:17:DF:35:E1:20	-59	-84	13
ISPoint01	00:0F:F8:58:E7:72	-90	-90	7

měření: místnost 207e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint08	00:17:DF:35:E0:70	-90	-90	1
ISPoint07	00:17:DF:35:E1:20	-64	-88	13
ISPoint06	00:17:DF:35:CE:20	-51	-61	11
ISPoint09	00:17:DF:35:CD:70	-86	-90	3
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint12	00:1C:B0:E8:31:00	-90	-90	5

měření: místnost 208e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint09	00:17:DF:35:CD:70	-72	-90	3
ISPoint01	00:0F:F8:58:E7:72	-87	-90	7
ISPoint02	00:0E:D7:C3:42:A0	-87	-90	7
ISPoint08	00:17:DF:35:E0:70	-90	-90	1
ISPoint07	00:17:DF:35:E1:20	-64	-90	13
ISPoint06	00:17:DF:35:CE:20	-33	-52	11

měření: místnost 209e

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint01	00:0F:F8:58:E7:72	-70	-90	7
ISPoint09	00:17:DF:35:CD:70	-81	-90	3
ISPoint06	00:17:DF:35:CE:20	-52	-68	11
ISPoint02	00:0E:D7:C3:42:A0	-83	-90	7
ISPoint07	00:17:DF:35:E1:20	-68	-90	13
ISPoint08	00:17:DF:35:E0:70	-90	-90	1
ISPoint10	00:17:DF:35:CC:80	-90	-90	8

měření: místnost 223a

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint10	00:17:DF:35:CC:80	-67	-90	8
ISPoint09	00:17:DF:35:CD:70	-70	-90	3
ISPoint02	00:0E:D7:C3:42:A0	-70	-90	7
ISPoint13	00:1C:B0:E8:33:80	-79	-90	1
ISPoint04	00:0F:F8:58:FF:F7	-90	-90	7
ISPoint01	00:0F:F8:58:E7:72	-90	-90	7

měření: místnost 225a

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint03	00:0F:F8:58:F4:D5	-68	-90	7
ISPoint10	00:17:DF:35:CC:80	-53	-70	8
ISPoint09	00:17:DF:35:CD:70	-90	-90	3
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7

měření: místnost 227

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint10	00:17:DF:35:CC:80	-62	-82	8
ISPoint09	00:17:DF:35:CD:70	-90	-90	3
ISPoint01	00:0F:F8:58:E7:72	-90	-90	7
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7

měření: místnost 227a

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint10	00:17:DF:35:CC:80	-51	-76	8
ISPoint09	00:17:DF:35:CD:70	-90	-90	3
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint03	00:0F:F8:58:F4:D5	-90	-90	7
ISPoint01	00:0F:F8:58:E7:72	-90	-90	7

měření: místnost 230s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint03	00:0F:F8:58:F4:D5	-35	-90	7
ISPoint10	00:17:DF:35:CC:80	-75	-90	8
ISPoint05	00:0F:F8:58:FF:FA	-90	-90	7

měření: místnost 232s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint10	00:17:DF:35:CC:80	-90	-90	8
ISPoint05	00:0F:F8:58:FF:FA	-68	-90	7
ISPoint03	00:0F:F8:58:F4:D5	-61	-90	7

měření: místnost 233s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint03	00:0F:F8:58:F4:D5	-58	-90	7
ISPoint05	00:0F:F8:58:FF:FA	-68	-90	7
ISPoint04	00:0F:F8:58:FF:F7	-90	-90	7
ISPoint10	00:17:DF:35:CC:80	-83	-90	8

měření: místnost 234s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint05	00:0F:F8:58:FF:FA	-77	-90	7
ISPoint04	00:0F:F8:58:FF:F7	-90	-90	7
ISPoint03	00:0F:F8:58:F4:D5	-73	-90	7

měření: místnost 235s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint05	00:0F:F8:58:FF:FA	-60	-90	7
ISPoint04	00:0F:F8:58:FF:F7	-68	-90	7
ISPoint10	00:17:DF:35:CC:80	-90	-90	8
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7

měření: místnost 236s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint05	00:0F:F8:58:FF:FA	-70	-90	7
ISPoint04	00:0F:F8:58:FF:F7	-90	-90	7
ISPoint10	00:17:DF:35:CC:80	-84	-90	8
ISPoint03	00:0F:F8:58:F4:D5	-62	-90	7

měření: místnost 243s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint10	00:17:DF:35:CC:80	-66	-90	8
ISPoint05	00:0F:F8:58:FF:FA	-69	-90	7
ISPoint04	00:0F:F8:58:FF:F7	-85	-90	7
ISPoint13	00:1C:B0:E8:33:80	-90	-90	1
ISPoint03	00:0F:F8:58:F4:D5	-90	-90	7

měření: místnost 244s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint10	00:17:DF:35:CC:80	-75	-90	8
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint04	00:0F:F8:58:FF:F7	-63	-90	7
ISPoint09	00:17:DF:35:CD:70	-90	-90	3
ISPoint13	00:1C:B0:E8:33:80	-90	-90	1
ISPoint01	00:0F:F8:58:E7:72	-90	-90	7
ISPoint03	00:0F:F8:58:F4:D5	-90	-90	7
ISPoint05	00:0F:F8:58:FF:FA	-83	-90	7

měření: místnost 244sa

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint05	00:0F:F8:58:FF:FA	-72	-90	7
ISPoint04	00:0F:F8:58:FF:F7	-68	-90	7
ISPoint10	00:17:DF:35:CC:80	-69	-90	8
ISPoint13	00:1C:B0:E8:33:80	-90	-90	1
ISPoint09	00:17:DF:35:CD:70	-83	-90	3
ISPoint01	00:0F:F8:58:E7:72	-90	-90	7

měření: místnost 245s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint10	00:17:DF:35:CC:80	-77	-90	8
ISPoint09	00:17:DF:35:CD:70	-90	-90	3
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint04	00:0F:F8:58:FF:F7	-55	-82	7
ISPoint08	00:17:DF:35:E0:70	-90	-90	1
ISPoint13	00:1C:B0:E8:33:80	-77	-90	1
ISPoint05	00:0F:F8:58:FF:FA	-77	-90	7
ISPoint03	00:0F:F8:58:F4:D5	-90	-90	7

měření: místnost 255s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint02	00:0E:D7:C3:42:A0	-88	-90	7
ISPoint05	00:0F:F8:58:FF:FA	-90	-90	7
ISPoint04	00:0F:F8:58:FF:F7	-37	-64	7
ISPoint13	00:1C:B0:E8:33:80	-90	-90	1
ISPoint03	00:0F:F8:58:F4:D5	-90	-90	7

měření: místnost 256s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint02	00:0E:D7:C3:42:A0	-75	-90	7
ISPoint04	00:0F:F8:58:FF:F7	-35	-57	7
ISPoint05	00:0F:F8:58:FF:FA	-90	-90	7

měření: místnost 257s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint04	00:0F:F8:58:FF:F7	-31	-63	7
ISPoint05	00:0F:F8:58:FF:FA	-90	-90	7
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7

měření: místnost 258s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint04	00:0F:F8:58:FF:F7	-38	-71	7
ISPoint13	00:1C:B0:E8:33:80	-90	-90	1

měření: místnost 262s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7
ISPoint05	00:0F:F8:58:FF:FA	-66	-90	7
ISPoint04	00:0F:F8:58:FF:F7	-66	-90	7
ISPoint03	00:0F:F8:58:F4:D5	-90	-90	7

měření: místnost 264s

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint04	00:0F:F8:58:FF:F7	-57	-69	7
ISPoint05	00:0F:F8:58:FF:FA	-90	-90	7
ISPoint02	00:0E:D7:C3:42:A0	-90	-90	7

měření: parkoviště střed

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint09	00:17:DF:35:CD:70	-90	-90	3
ISPoint02	00:0E:D7:C3:42:A0	-67	-84	7
ISPoint07	00:17:DF:35:E1:20	-90	-90	13
ISPoint04	00:0F:F8:58:FF:F7	-90	-90	7

měření: parkoviště východ

SSID	MAC	RSSI [dB]		k.
		max		
ISPoint09	00:17:DF:35:CD:70	-84	-90	3
ISPoint06	00:17:DF:35:CE:20	-61	-70	11
ISPoint02	00:0E:D7:C3:42:A0	-68	-80	7
ISPoint08	00:17:DF:35:E0:70	-60	-90	1
ISPoint07	00:17:DF:35:E1:20	-58	-69	13
ISPoint12	00:1C:B0:E8:31:00	-73	-90	5
ISPoint13	00:1C:B0:E8:33:80	-90	-90	1

měření: parkoviště západ

SSID	MAC	RSSI [dB]		k.
		ma x		
ISPoint02	00:0E:D7:C3:42:A0	-67	-90	7
ISPoint04	00:0F:F8:58:FF:F7	-65	-90	7
ISPoint05	00:0F:F8:58:FF:FA	-90	-90	7

Příloha č. 2- Přehled bezdrátových bodů a jejich umístění

Jméno	Umístění	Frekvence
ISPoint1	Komín	2,4 GHz
ISPoint2	Chodba 2 stupeň ZŠ a SŠ	2,4 GHz
ISPoint3	Jídelna, Kancelář ředitelky ZŠ	2,4 GHz
ISPoint4	Chodba 2 stupeň ZŠ	2,4 GHz
ISPoint5	Střední škola	2,4 GHz
ISPoint6	Přízemí 1 stupeň ZŠ a třída 117	2,4 GHz
ISPoint7	1 stupeň ZŠ – 4 a 5 třídy	2,4 GHz
ISPoint8	1 stupeň ZŠ – 4 a 5 třídy	2,4 GHz
ISPoint9	1 stupeň ZŠ – 4 a 5 třídy, Admin	2,4 GHz
ISPoint10	Chodba SŠ a Knihovna	2,4 GHz
ISPoint11	Školka	2,4 GHz nebo 5 GHz
ISPoint12	1 stupeň ZŠ – 1 a 2 třídy	2,4 GHz nebo 5 GHz
ISPoint13	Divadlo	2,4 GHz nebo 5 GHz

Zdroj: Vlastní