Návrh a realizace bezdrátových sítí

Wireless System Design

Martin Vašek

Bakalářská práce
2009

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav aplikované informatiky
akademický rok: 2008/2009

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Martin VAŠEK**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Návrh a realizace bezdrátových sítí**

Zásady pro vypracování:

1. **Vypracujte literární rešerší zaměřenou na bezdrátové sítě.**
2. **V rámci literární rešerše se zaměřte na technické prostředky bezdrátových sítí, jejich správu a konfiguraci.**
3. **Navrhněte a realizujte konkrétní bezdrátovou síť.**
4. **Ověřte dosah signálu v dané síti a prostupnost signálu v konkrétních terénních podmínkách.**
5. **Popište způsob zabezpečení bezdrátové sítě a typy možných útoků na ní.**

Rozsah práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **HORST, J.: Informační a telekomunikační technika. Praha, BEN, 2004. ISBN: 8086706087.**
2. **KLAUS, T: Příručka pro elektrotechnika. Europa – Sobotáles, 2005. ISBN: 8086706001.**
3. **KOMAR, B.: Zabezpečení systému a sítě. Computer Press, 2007.ISBN: 8025112608.**
4. **PUŽMANOVÁ, R.:Moderní komunikační sítě od A do Z.Computer Press,2006. ISBN: 8025112780.**
5. **HORSKÝ, R.: Bezdrátové sítě Wi-Fi v rekordním čase. Grada, 2006. ISBN: 8024717905.**

Vedoucí bakalářské práce: **doc. Mgr. Milan Adámek, Ph.D.**
Ústav elektrotechniky a měření

Datum zadání bakalářské práce: **20. února 2009**

Termín odevzdání bakalářské práce: **1. června 2009**

Ve Zlíně dne 13. února 2009

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Ing. Ivan Zelinka, Ph.D.
ředitel ústavu

Poděkování,motto

Velké poděkování patří vedoucímu mé práce Mgr.Milanovi Adámkovi,Ph.D. a současně také konzultantu mé práce panu Petru Cholastovi.Jejich trpělivost,ochota a pomoc byly základem pro zpracování mé bakalářské práce.Díky jejich teoretickým znalostem praktickým zkušenostem,cenným radám a připomínkám se práce na bakalářské práci pro mne stala zdrojem získání velmi kvalifikovaných informací,nových zkušeností a hlavně návodů na pracovní postupy při samotném zpracování projektů.

Prohlašuji, že jsem na bakalářské/diplomové práci pracoval(a) samostatně a použitou literaturu jsem citoval(a). V případě publikace výsledků, je-li to uvedeno na základě licenční smlouvy, budu uveden(a) jako spoluautor(ka).

Ve Zlíně

.....
Podpis diplomanta

Abstrakt

Bakalářská práce je zaměřená na návrh,správu,zabezpečení a konfigurací bezdrátových sítí, především pak sítích založených na normách IEEE 802.11, neboli WiFi (Wireles Fidelity). Literární rešerše popisuje krátkou historii vývoje bezdrátových sítí. Následuje podrobný popis normy 802.11 a jejich služeb. Dále je uveden přehled aktivních a pasivních prvku WiFi sítí. Další kapitola se zabývá především správou a konfigurací WiFí sítí, jsou zde popsány nejdůležitější služby a možnosti jejich konfigurace. Neopomenutelnou problematikou je bezpečnost WiFi sítí, proto je ji také věnovaná samostatná kapitola, ve které jsou popsány základní bezpečnostní mechanizmy. Na závěr, je uvedena praktická ukázka konfigurace přístupového bodu a klientské stanice.

Klíčová slova

LAN, MAN, WAN, rozprostřené spektrum, peer-to-peer sítě, serverové sítě, WLAN, IEEE 802.11, Bluetooth, HiperLAN, WinMax, WiFi, model OSI, topologie WiFi sítí, přístupový bod, síťový adaptér, anténa, DHCP server, NAT, filtrování, firewall, přesměrování portů, VPN, WEP, EAP, autentizace, šifrování, WPA.

Obsah

1 Úvod

První bezdrátové sítě se začali objevovat po roce 1992. Zařízení bezdrátových sítí pracovala s přenosovými rychlostmi, které nedosahovaly ani zlomku rychlostí současných bezdrátových sítí. Dalším závažným problémem bylo, že chyběla jakákoliv standardizace bezdrátové komunikace, což mělo za následek, že každý výrobce si vyráběl vlastní bezdrátová zařízení, která nebyla mezi sebou navzájem kompatibilní.
To se změnilo v červenci roku 1997, kdy byl schválen standard pro bezdrátové sítě IEEE 802.11, pro který se začalo používat označení WiFi (Wireless Fidelity). Postupem času k původnímu standardu vzniklo a vzniká řada dalších nových norem, doplňků a revizí.
Zavedení standardu do bezdrátové komunikace založené na normě IEEE 802.11 vedlo k velkému rozvoji tohoto odvětví. Vzájemná kompatibilita jednotlivých zařízeni přispěla k větší konkurenci mezi výrobci, k postupnému snižování cen a v poslední době tak 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 přenosové medium radiové vlny, podobně jako například sítě mobilních operátorů nebo radiové a televizní vysílaní. Všechny tyto sítě mají společný znak, k jejich provozování musí mít provozovatel licenci vydávanou patřičným regulačním úřadem. Každý vlastník licence dostává od regulátora přiděleno svoje frekvenční pásmo, na kterém může provozovat vysílaní. Bezdrátové sítě 802.11 využívají bezlicenční pásmo 2,4 GHz a 5 GHz. To znamená, že při dodržení pravidel nastavených regulátorem, může každý provozovat bezdrátovou radiovou síť v bezlicenčním pásmu.
WiFi sítě svým uživatelům nabízejí několik zásadních výhod, které jistě přispěly k velkému rozšíření těchto sítí. Mezi zásadní patří především možnost snadno vytvořit počítačovou síť bez nutnosti pokládky kabelů. Další výhodou je zavedení jednotného standardu pro WiFi zařazení a použití bezlicenčního pásma. Příznivé ceny vedly k tomu, že uživatele začali zakládat často velmi rozsáhlé komunitní sítě, pomocí nichž mohli sdílet data, hrát hry a především sdílet širokopásmové připojení k internetu.
Tato práce by měla poskytnout základní přehled bezdrátových sítích 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 domácí uživatele a malé firmy.

2 Cíl práce a metodika

Bakalářská práce se zabývá návrhem, správou, zabezpečením a konfigurací konkrétní bezdrátové sítě,založené na normách IEEE 802.11, neboli WiFi (Wireles Fidelity). Literární rešerše popisuje krátkou historii vývoje bezdrátových sítí. Následuje stručný popis normy 802.11. Dále uvádím přehled aktivních a pasivních prvku WiFi sítě. Další kapitola se zabývá především správou a konfigurací WiFí sítí, jsou zde popsány důležitější služby a možnosti jejich konfigurace.Dále popisuji problematiku zabezpečení a typy možných útoků na ní.Závěrem se věnuji praktické ukázce konfigurace přístupového bodu a klientské stanice.

3 Počítačové sítě

(6) Síť je spojením určitého hardwaru,softwaru a kabelů(vodičů),které společně umožňují vzájemnou komunikaci různých počítačových zařízení.
Pokud jsou počítače propojené s dalšími počítači a sdílejí společné prostředky, označujeme tuto skupinu počítačů jako počítačovou síť. Přitom není podstatné zda jde o prostředky softwarové či hardwarové.

Počítače mohou sdílet:

- Data
- Zprávy
- Grafiku
- Tiskárny
- Faxové přístroje
- Modemy
- Další hardwarové zdroje

S rostoucím vývojem informačních technologií se tento seznam neustále rozšiřuje

3.1 Typy sítí

Počítačové sítě můžeme rozdělit z více hledisek. Jedním z nich je rozdělení dle rozlehlosti a účelu a to na sítě **LAN, MAN, WAN a PAN**.
Dále lze počítačové sítě rozdělit na sítě typu **peer-to-peer** a **serverové sítě**.

3.1.1 LAN

Dnešní moderní sítě LAN (Local Area Network - Lokální sítě) propojují širokou škálu počítačů a dalších zařízení. Jednotlivé LAN sítě se pak navzájem propojují do větších celků.

Přenosové rychlosti LAN sítí se pohybují od desítek Mbit/s až po jednotky Gbit/s.

(11) Mezi LAN sítě patří

- Ethernet, Fast Ethernet, Gigabit Ethernet (IEEE 802.3)
- Arc net
- Token Bus (IEEE 802.4)
- Token Ring (IEEE 802.5)
- IsoEthernet (IEEE 802.9)
- Bezdrátové sítě (WiFi, 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

MAN (Metropolitan Area Network) je označení pro metropolitní sítě. Propojují lokální sítě v městské zástavbě, slouží pro přenos dat, hlasu a obrazu. Spojují počítače na vzdálenost řádově jednotek až desítek km.

Přenosová rychlost bývá vysoká a vychází z rychlostí LAN sítí.

(11) Mezi MAN sítě patří

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

3.1.3 WAN

Je počítačová síť, která pokrývá rozlehlé geografické území (například síť, která překračuje hranice města, regionu nebo státu).
Počet uživatelů takovéto sítě může jít do milionů (např. internet).

Přenosová rychlost WAN sítí se pohybuje od desítek Kbit/s až řádově stovek Gbit/s.

(11) Mezi WAN sítě patří

- Integrated Services Digital Network (ISDN)
- X25
- Frame Relay
- Switched Multimegabit Data Service (SMDS)
- Asynchronous Transfer Mode (ATM)
- Wimax (IEEE 802.16d)

3.1.4 PAN

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

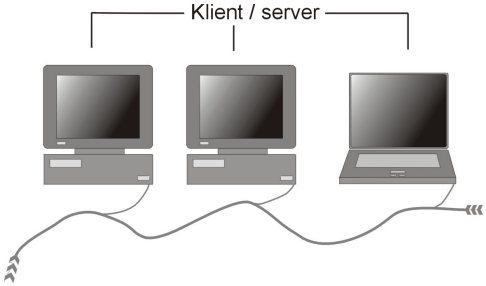
Rychlost PAN sítí zpravidla nepřekračuje jednotky Mbit/s. Pro tyto sítě je důležitější odolnost proti rušení, nízká spotřeba a snadná konfigurovatelnost.

(11) Mezi PAN sítě řadíme

- Bluetooth
- Zigbee
- IrDA

3.1.5 Sítě typu peer-to-peer

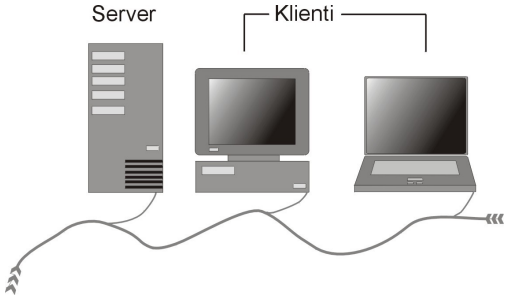
(6) Tyto sítě vycházejí z toho, že všechny počítače zapojené v této síti jsou si rovny. To znamená, že v této síti neexistuje hierarchie počítačů. Všechny počítače fungují jako klient i server. Každý jednotlivý uživatel určuje, která data poskytne ke sdílení tj. klienti uživatelé komunikují přímo mezi sebou.
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 a to zejména díky tomu, že umožňují snadnou výměnu dat.



Obrázek 3.1: Síť typu peer-to peer

3.1.6 Serverové sítě

(7) Sítě, kde jeden počítač (nebo více počítačů) je vyhrazen jako server. Takový počítač se nepožívá jako klient nebo pracovní stanice, ale je optimalizován na to, aby zajistil rychlou obsluhu klientů a zajistil ochranu sdílení souborů a adresářů. S rostoucím počtem počítačů připojených v síti roste i počet serverů a následně také jejich specializace, aby jejich úkoly byli provedeny co nejefektivněji.



Obrázek 3.2: Serverová síť

Základní typy serverů jsou:

- Souborové a tiskové servery – slouží k ukládání souborů a dat
- Aplikační servery – zpřístupňují klientům serverovou část aplikace
- Poštovní servery – zajišťují posílání elektronických zprav mezi uživateli sítě
- Komunikační servery – zajišťují posílání zprav mezi uživateli vlastní sítě a dalších sítí a nebo komunikaci vlastní sítě se vzdálenými uživateli například pomocí modemu

(6) Mezi výhody serverových sítí patří možnost centrální správy a kontroly. 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.

3.2 Bezdrátová komunikace

(5) Spočívá ve spojení dvou subjektů jiným způsobem, než mechanicky (kabelem). Většina bezdrátových sítí používá kabely k propojení bezdrátových komponent, částí svých segmentů a kabelové sítě.Takovéto kombinované sítě se také nazývají hybridní sítě.

3.2.1 Přenosové techniky

Pro přenos dat se u bezdrátových sítí využívají různé techniky. V následujícím přehledu budou obsaženy některé z nejvýznamnější technik bezdrátové komunikace a jejich stručné charakteristiky.

3.2.1.1 Infračervené záření, IrDA

(11) 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.

3.2.1.2 Laser

(11) V současné době se pro komunikaci pomocí laseru využívá dvousměrných teleskopů s rychlými transceivery, které mohou dosahovat rychlost až 2,5 GB/s. Při použití této technologie je nutné, aby byla provozovatelem zajištěna přímá viditelnost mezi optickými jednotkami. Funkčnost a spolehlivost takovýchto linek v případě dostatečné výkonové rezervy neohrožuje déšť ani sněžení, avšak fatální následky na funkčnost má mlha. To se dá částečně eliminovat umístěním teleskopů na střechy výškových budov či případným zálohováním komunikace pomocí radiové sítě, na které mlha nemá vliv.

3.2.1.3 Radiové frekvence

Technologie založené na komunikaci pomocí radiových vln patří mezi nejrozšířenější a nejvíce využívané. Většina radiových přenosů může probíhat na vzdáleností několika stovek až tisíce metrů a není omezena přímou viditelností.

3.2.2 Přehled bezdrátové radiové technologie

3.2.2.1 Frekvence

(10) Bezdrátové sítě využívající radiové vlny pracují ve stanovených frekvencích. Používání radiofrekvenčních pásem však podléhá regulaci ze strany státních úřadů. V případě České republiky tato regulace podléhá ČTÚ (Český telekomunikační úřad www.ctu.cz). Většina vysílacího spektra podléhá licencím, například ty, co využívají provozovatelé k televiznímu a rozhlasovému vysílaní nebo spektrum, které využívají mobilní operátoři. Z tohoto důvodu musí WiFi sítě využívat jednoho ze dvou nelicencovaných pásem:

- **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 (75) kanálů, Evropa)

(12) Pásmo 5 GHz je velmi nepřehledné, má několik subpásem, které mají rozdílnou regulaci:

- **5150-5250 MHz** – Povoleno v Americe i Evropě, avšak pouze pro vnitřní sítě s max. 200 mW EIRP (Effective isotropically-radiated power), od 1. 9. 2005 také v ČR. Toto pásmo je podporováno standardy IEEE 802.11a a 802.11h.
- **5250-5350 MHz** – Povoleno v Americe i Evropě, avšak pouze pro vnitřní sítě s max. 1 W EIRP (Amerika) a max. 200 mW EIRP (Evropa), od 1. 9. 2005 také v ČR . Toto pásmo je podporováno standardy IEEE 802.11a a 802.11h.
- **5470-5725 MHz** – V Americe se připravuje uvolnění tohoto pásma, v Evropě se tak již stalo - pro venkovní i pro vnitřní sítě s max. výkon 1 W EIRP. V ČR je od 1. 9. 2005 nejvyšším povoleným subpásmem pro volné použití. Toto pásmo ovšem nespecifikuje žádný IEEE standard.
- **5725-5825 MHz** – V Americe je v tomto pásmu možno vysílat venku i uvnitř budov s max. 4 W EIRP, v Evropě včetně ČR jen v rámci nespecifikovaných stanic s maximálním vyzářeným výkonem 25 mW. Opět není podporováno IEEE standardy.
- **5825-5875 MHz** – Povoleno v Evropě včetně ČR jen v rámci nespecifikovaných stanic s maximem 25 mW vyzářeného výkonu. Není podporováno IEEE standardy.

3.2.2.2 Spektrum

(10) Přestože ve frekvenčních pásmech 2,4 a 5 GHz není potřeba žádná licence, ČTÚ zavádí určitou regulaci. Tato pravidla mají zabránit tomu, aby bezdrátové přenosy nevyužívali nadměrnou šířku pásma a nepoužívali příliš velký výkon vysílaní. To by mohlo způsobovat rušení jiných signálů, které využívají tyto pásma.
Další pravidlo, které ČTU vyžaduje, je používání jedné ze tří technologií rozprostřeného spektra.

Rozprostřené spektrum

(10) 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.

Technologie rozprostřeného spektra

- (10) **DSSS** (Direct Sequence Spread Spectrum) Rozprostřené spektrum v přímé posloupnosti rozprostírá signály přes několik kanálů v určitém frekvenčním rozsahu. Binární řetězec nazývaný *kód prostředí* vytváří redundanci. Signál je rozprostřen do většího radiového spektra, je méně citlivý vůči rušení, což zajišťuje větší spolehlivost signálu. Jedná se o modulační techniku používanou například v bezdrátové technologii WiFi či v navigačním systému GPS.

- (10) **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. chybně přenesené rámce) jsou přeneseny znovu s jinou nosnou frekvencí. Další výhodou je možnost umístění více systémů v jednom místě, použitím různých frekvencí v každém systému .

- (10) **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.

3.2.3 Hlavní normy radiokomunikačních bezdrátových sítí

3.2.3.1 IEEE 802.11

(10,12) The Institute of Electrical and Electronics 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 rychlosti, odlišnou metodu rozprostřeného spektra a pracovala ve frekvenčním pásmu 5 GHz. V roce 2002 přibyla další norma 802.11g. IEEE schválilo poté další normu v oblasti bezdrátových lokálních sítí. Nejednalo se o čtvrtý typ, ale o doplněk ke specifikaci 802.11a určenou pro použití v Evropě.

Přehled základních norem 802.11

802.11b
(10,12) 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 Air-Port. Sada se skládala z bezdrátového přístupového bodu a PC karty pro notebooky Macintosh. Díky tomu se technologie bezdrátových sítí značně zpopularizovala a rozšířila mezi širokou veřejnost. V dnešní době patří norma IEEE 802.11b stále mezi nejvíce rozšířené především z hlediska dostupnosti zařízení založených na této normě a oblíbeností mezi uživateli.
Sítě založené na normě 802.11b pracují s maximální přenosovou rychlostí 11 Mbit/s a využívají rozprostřeného spektra DSSS.

802.11a
(10,12) Norma IEEE 802.11a byla schválena brzy po normě 802.11b v roce 1999. Práce na této normě začali sice jíž 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.

802.11g
(10,12) 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.

Typ	Frekvence [GHz]	Přenosová rychlost [Mbit/s]	Reálna rychlost [Mbit/s]	Rozprostřené spektrum
802.11b	2,412 – 2,484	11	6	DSSS
802.11g	2,412 – 2,484	54	22	OFDM/DSSS
802.11a	5,150 - 5,350 a 5,725 - 5,825	54	25	OFDM

Přehled základních norem standardu 802.11

Doplňující normy 802.11

V předchozím přehledu byli představeny základní normy týkající se WiFi, které lze považovat za stěžejní a na základě nichž se vyvinuly nebo jsou připravovány další normy. V následujícím přehledu jsou uvedeny některé z nich.

802.11e
(12) Tato norma zavádí podporu služby 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.. Dále nahrazuje stávající metody pro přístup k mediím a zajišťuje zpětnou kompatibilitu se zařízeními, které QoS nepodporují.
Norma ještě nebyla dosud schválena.

802.11f
(12) 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.
Norma byla schválena v roce 2003.

802.11h
(12) Norma 802.11h zavádí použití dynamického výběru kanálů DCS (Dynamic Channel Selection) a řízení vysílacího výkonu TPC (Transmit Power Control) u zařízení pracujících v kmitočtovém pásmu 5 GHz (tj. doplňuje normu IEEE 802.11a). Díky tomuto doplňku lze zabránit nepříznivému vlivu normy IEEE 802.11a na radarové systémy a průzkumné satelitní systémy.
Norma byla schválena v roce 2003.

802.11i
(12) Norma 802.11i zavádí nové bezpečnostní 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.
K nedostatkům v bezpečnosti protokolu WEP (Wired Equivalent Privacy) patří nedostatečná autetizace a slabé šifrování statickým klíčem.

Autentizace je v této normě prováděna výrazně kvalitněji za použití obecného rámce řízení přístupu podle 802.1x (Port-Based Network Access Control), EAP (Extensible Authentication Protocol) a alternativně přednastaveného sdíleného klíče PSK (Pre-Shared Key). Pro šifrování je místo WEP použit nově vytvořený protokol pro šifrování dynamickým klíčem, TKIP (Temporal Key Integrity Protocol) a zavedl se také management klíčů. Navíc se kontroluje integrita zpráv pomocí algoritmu označovaného Michael (MIC, Message Integrity Check).
Dalším výrazným přínosem této normy, je zavedení nového šifrovacího mechanizmu AES (Advanced Encryption Standard), který na rozdíl od původního mechanizmu RC4, který se používal ve WEP protokolu, nabízí kvalitnější způsob šifrování a tím i větší bezpečnost. S tímto šifrováním je možné sítě označit za bezpečné a využívat je i pro velmi citlivé účely (např. banky, vládní instituce atp.).
Norma byla schválena v roce 2004.

802.11k
(12) Norma 802.11k je připravovaná s cílem zefektivnit přenosy na základě měření kvality jednotlivých kanálů, šumu zahlcení a vzájemného rušení. Norma by měla umožnit jednotlivým přístupovým bodům vyměňovat si hodnoty měření kvality signálů a tím jim umožnit přizpůsobit výkon, využívat nezatížené kanály a tak zajistit efektivnější přenosy.

802.11n
(12) Norma 802.11n přinesla revoluční zvýšení přenosových rychlostí. Cílem normy 802.11n je nabídnout uživatelům rychlosti dosahující minimálně 100 Mbit/s, v ideálním případě až 600 Mbit/s. Tohoto nárůstu přenosových rychlostí se dosáhne využitím více antén a změnou kódovacích schémat MAC protokolů.

3.2.3.2 Bluetooth

(10,11) Bluetooth je bezdrátová radiokomunikační technologie pracující v 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. Tato verze je používána v drtivé většině současných zařízeních využívajících Bluetooth. Datová propustnost se pohybuje kolem 1 Mbit/s. V současné době se připravuje nová specifikace Buetooth 2.0 ERD, která by měla přenosové rychlosti zvýšit až na trojnásobek současného maxima.
Bluetooth je určena především k bezdrátovému propojení počítače s jinými periferními zařízeními jako jsou například mobilní telefony, PDA atp..

3.2.3.3 HiperLAN

(1) 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 verze pracují ve frekvenčním pásmu 5 GHz a dosahují přenosových rychlostí v případě starší verze 24Mbit/s a v případě novější normy 54MBit/s.
Na rozdíl od sítí 802.11 HiperLAN podporuje kvalitu služeb pro přenos hovorových signálů a videa tzv. QoS, poskytuje kvalitní zabezpečení, efektivně řídí spotřebu energie bezdrátových zařízení, a umožňuje snadnou autokonfiguraci.
I přes to, že HiperLAN poskytuje svým uživatelům některé výhody oproti normám 802.11 jeho další vývoj je nejistý z důvodů nechuti výrobců vyrábět cokoliv jiného než jsou zařízení standardu 802.11b respektive 802.11g.

3.2.3.4 WinMax

(11) WinMax (Worldwide Interoperability for Microwave Access) představuje bezdrátovou technologii určenou pro spojení na dlouhou vzdálenost a umožňující vysokou datovou propustnost. WinMax 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.
První verze standardu 802.16 byla schválena v roce 2002. Pracovala v pásmu 10-66 GHz a byla nutná přímá viditelnost mezi vysílačem a přijímačem. Přenosové rychlosti dosahovali 134 Mbit/s.
V dubnu roku 2003 byla schválená nová verze standardu 802.16, která pracuje v pásmu 2-11 GHz. To znamená, že pokrývá jak licencované tak bezlicenční pásmo. Přenosová rychlost oproti původní normě klesla na polovinu tj. 70 Mbit/s. Dosah sítí založených na této normě je 40 až 70 km a není nutná přímá viditelnost.
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 WinMax se neustále pracuje a tak v nejbližší době by se uživatelé těchto sítí měli dočkat také mobilních zařízeních na tomto standardu v podobě přídavných karet do notebooku atp.. Zařízení založené na technologii WinMax 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 WinMaxu jako velmi slibná.

3.2.4 WiFi

(10,12) 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 používaní loga na jejich zařízeních a marketingových materiálech.
Logo WiFi představuje záruku toho, že takto označené výrobky by neměl být problém propojit mezi sebou.

Obrázek 3.3: Logo WiFi Alliance zaručující kompatibilitu. Barevné oválné značky s písmeny dále zpřesňují, které standardy zařízení splňuje

V poslední době se termín WiFi používá pro označení všech sítí založených na standardu IEEE 802.11, což sice není přesné (ne všechna zařízení musí vyhovovat podmínkám WiFi Aliance), ale už je na tolik vžité, že je chápáno jako ekvivalent k sítím standardu IEEE 802.11a/b/g.

3.3 Podrobný popis IEEE 802.11

Pochopení normy 802.11 je důležité při stavbě sítí které jsou na této normě založené. Dále pomůže při posuzování (ne)výhod, které sítě WiFi nabízejí.

Základní součásti WiFi sítě
(1) 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 pro 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 je vybaven radiovým zařízením podobně jako síťová stanice.
Aby WiFi stanice a přístupové body mezi sebou mohli úspěšně komunikovat musí využívat stejnou normu pro komunikaci bezdrátových sítí, nebo normy mezi sebou navzájem kompatibilní.

3.3.1 IEEE 802.11 a model OSI

(1) 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.
Komunikace mezi vrstvami se zpravidla řídí pravidly, která se nazývají rozhraní (interface) a komunikace mezi vrstvami různých systému se řídí protokoly. Normy IEEE 802 pracují na fyzické a síťové vrstvě jako 802.3 (běžně označovaný jako

Ethernet) a 802.11 (bezdrátový protokol označován jako WiFi). Protokoly vyšších vrstev referenčního modelu jsou například TCP/IP, NETBIOS a mnoho dalších. Tyto protokoly jsou zcela nezávislé na nižších vrstvách a používají nižší vrstvy jako platformu, na které pracují.
Normy IEEE 802.11 umožňují použití různých verzí nějaké konkrétní vrstvy v rámci OSI.
Vrstvy se také často člení do podvrstev, které přebírají jen určitou část práce vrstvy. Rozdělení vrstvy na podvrstvy umožňuje sítím, které jsou jinak odlišné používat společnou podvrstvu.

(9) **Vrstvy ISO/OSI**

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

3.3.1.1 Fyzická vrstva

(9) Fyzická vrstva je nejnižší vrstvou v referenčním modelu OSI. Struktura vrstvy v modelu 802.11 je rozdělena do dvou podvrstev:

- Protokol konvergence fyzické vrstvy (PLCP, Physical Layer Convergence Procedure)

- Podvrstva závislá na fyzickém mediu (PMD, Physical Medium Dependent)

(9) PLCP představuje spojení mezi přenášenými rámci MAC podvrstvy a přenosovým mediem. Podvrstva PLCM připojuje k přenášeným rámcům vlastní hlavičky v závislosti na použité metodě modulace. Dále poskytuje funkci CCA (Clar Channel Assessment), odezvu pro podvrstvu MAC, že přenosové medium je k dispozici. Díky této funkci je možné pro standard 802.11 používat různá přenosová media. V současnosti se využívá radiové spektrum a infračervené světlo.
PMD se stará o kódování bezdrátového přenosu a o přenos každého jednotlivého bitu z podvrstvy PLCP do éteru pomocí antény.

3.3.1.2 Vrstva řízení přístupu k mediu MAC

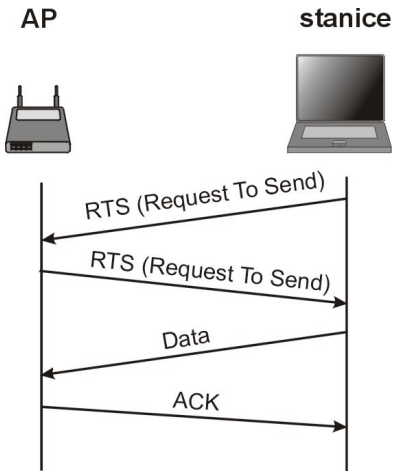
(9) Důležitou vrstvou bezdrátové sítě 802.11 je podvrstva spojové vrstvy MAC (Medium Access Control), nebo také vrstva řízení přístupu k médiu.
Pro robustnost podvrstvy MAC jsou důležité dvě hlavní vlastnosti. Každý přenášený paket je opatřen kontrolním součtem CRC (Cyclic Redundancy Check), díky tomu je

možné poznat zda (ne)byl během přenosu poškozen. Další vlastností je fragmentace paketů, která rozděluje přenášené pakety do menších celků a přenáší je postupně.

MAC podvrstva standardu 802.11b je velmi podobná 802.3 ethernetovému standardu. U ethernetu se používá protokol CSMA/CD (systém detekce kolizí), naproti tomu standard 802.11 definuje CSMA/CA (systém předcházení kolizím), protože u bezdrátového media se obtížně detekují kolizní stavy.
CSMA/CD (Collision Detection - Detekce kolizí) technologii používá klasický ethernet. Použití pro WiFi není možné, protože nelze přijímat a současně odesílat přenosy z jedné radiové stanice (tj. musel by být realizován plně duplexní radiový kanál). Další věc, která zabraňuje použití této technologie pro WiFi je, že při komunikaci vzdálených stanic není tato komunikace zachytitelná pro danou stanici.
CSDMA/CA (Collision Avoidance – Předcházení kolizí) technologie využívá potvrzovacího schématu a zabraňuje vzniku kolizí. Předpokládejme, že stanice chce vysílat a naslouchá na mediu a čeká, dokud nebude volné. Pokud je medium neobsazené, stanice počká ještě nějakou dobu (DIFS - Distributed Inter Frame Space) a pak začne vysílat. Po přenosu dat přijímací stanice zkontroluje CRC (Cyclic redundancy check) přijatého paketu a v případě, že je v pořádku odešle vysílací stanici ACK (Acknowledge) rámec, kterým vysílací straně potvrzuje, že paket byl přijat. Vysílací stanice vyhodnotí, že nedošlo ke kolizi a přenos proběhl v pořádku. V případě, že by stanice tento potvrzovací paket neobdržela dojde k novému pokusu o přenos, dokud se nevyčerpá určitý počet pokusů.

3.3.1.3 RTS/CTS

(9) Metoda RTS/CTS (Request to Send / Clear to Send) je mechanizmus jehož cílem je minimalizovat překrývající se přenosy v rušeném prostředí.
Stanice, která chce vysílat vyšle nejprve RTS (Ready to send) rámec, který obsahuje adresu příjemce, délku zprávy a dobu následujícího přenosu. Cílová stanice odpovídá zasláním CTS (Clear to send) paketem, který rovněž obsahuje dobu trvání přenosu. Na základě RTS nebo CTS rámce se v každém uzlu vypočte NAV (Network allocation vector), který upozorňuje ostatní uzly, že síť je na tuto dobu obsazena. Tímto mechanizmem se snižuje pravděpodobnost, že bude docházet ke kolizím ze strany ostatních stanic.
Mechanizmus RTS/CTS je nepovinný a zařízení standardu 802.11 jej nemusí implementovat.



Obrázek 3.4: Předcházení kolizím (RTS/CTS)

Vrstva MAC zajišťuje řadu služeb stanice, které se vztahují k tomu, jak mezi sebou bezdrátová zařízení komunikují. Dále také zajišťuje distribuční služby, které se vztahují ke komunikaci přístupových bodů.

3.3.1.4 Služby stanice 802.11 MAC

(10) **Autentizace** – Většina přístupových bodů je nastavena tak, že vyžadují autentizaci od zařízení, které se chce připojit do sítě. Jedním ze způsobů autentizace je tzv. otevřená autentizace, která umožňuje bez omezení se připojit do sítě. Naproti tomu může přístupový bod vyžadovat tzv. autentizaci se sdíleným klíčem. Přístupový bod bude vyžadovat sdílený klíč k připojení do sítě.

(10) **Deautentizace** – V případě odpojení stanice od sítě se provede služba deautentizace a přerušení spojení.

(10) **Utajení** – Norma 802.11b k zajištění bezpečnosti používá protokol WEP (Wires Equivalent Privacy), aby se zabránilo odposlouchávání dat ze vzduchu. K šifrování se používají 64-128 bitové klíče. Pro dešifrování se klient musí autentizovat do dané sítě a jako člen sítě obdrží přístupový klíč, na základě něhož data dešifruje.
Bližší pohled na bezpečnost WiFi komunikace je uveden v kapitole 5 (Bezpečnost sítí). Zde je také popsána nedostatečná bezpečnost protokolu WEP.

(10) **Předání** – Služba datové jednotky MAC (MSDU) zajišťuje, že data dorazí k zamýšlenému příjemci.

Distribuční služby 802.11 MAC

(10) **Přidružení** - Pokud je bezdrátová síť tvořena více přístupovými body je nutné, aby každá stanice byla přidružena k nějakému přístupovému bodu. Přístupové body předávají informace o přiřazení stanice na další části sítě.

(10) **Odpojení** – Dochází v případě, že se stanice vzdálí od přístupového bodu mimo jeho dosah, nebo přístupový bod ukončí spojení se stanicí a provede tak odpojení stanice od sítě.

(10) **Nové přidružení** – Služba se provádí, když mobilní stanice změní své přidružení k přístupovému bodu vlivem pohybu a přechodu od jednoho přístupovému bodu k druhému.

(10) **Distribuce** – Zajišťuje, aby data dorazila k cíli při posílaní informace z jedné stanice k druhé v rámci WiFi sítě.

(10) **Integrace** - Umožňuje zařízením WiFi komunikovat se sítěmi jiného typu než 802.11 (např. kabelové sítě) prostřednictvím portálu. Integrační služba vede data přes portál mimo WiFi síť.

3.3.1.5 Frekvenční spektrum

S technologií rozprostřeného spektra jsme se už krátce seznámily. V následujícím popisu standardu 802.11 si popíšeme funkci těchto metod.

3.3.1.5.1 DSSS (Direct Sequence Spread Spectrum)

(7) DSSS používá frekvenční pásmo 2400–2483 MHz. V tomto pásmu je umístěno 11 kanálů o šířce 22 MHz. Aby se kanály do pásma vešly, mají střední kmitočty od sebe posunuty pouze o 5 MHz. Je patrné, že nelze používat dvě zařízení DSSS na dvou sousedních kanálech, aby mezi nimi byl zachován odstup 22MHz. Minimální odstup dvou sousedních kanálů, při kterém je zachován odstup 22 (25) MHz je 5 kanálů.
Pro přenos dat se používá pseudonáhodný binární řetězec nazývaný čipový kód (chipping code). V tomto uspořádání několik bitů reprezentuje jeden bit informace. Tyto bity se přenášejí ve stejném intervalu, jaký by byl nutný k přenosu jednoho bitu.
Jinak řečeno každý bit je reprezentován obrazem několika bitů. 802.11 implementuje 11 bitový přenosový kód. Například nula je reprezentována kódem 11101100011 a jednička 00010011100. Kódy jsou navzájem inverzní, což zajišťuje vysokou odolnost proti rušení. Velikost kódu zajišťuje v případě chybného přenosu, že opravné techniky budou moci poškozená data rekonstruovat.

3.3.1.5.2 OFDM (Orthogonal Frequency Division Multiplexing)

(7,10) Metoda OFDM namísto vytváření velkého datového kanálu pro předání dat vysílá bity přes více podkanálů pracujících paralelně na různých frekvencích. OFDM umožňuje podobně jako paralelní zpracování u superpočítačů jednotlivým procesům se soustředit na určitý malý objem informací, nezatížený jinými úlohami. Na konci přenosu dojde ke složení dílčích kanálů dohromady (multiplexování). Výsledkem je vysoká propustnost.
Kanály OFDM se překrývají a používají jednoznačné identifikátory což zabraňuje případným interferencím. Úrovně rychlostí OFDM jsou 6 a 9 Mbit/s, 12 a 18 Mbit/s, 24

a 36 Mbit/s, 48 a 54 Mbit. První úroveň používá DBPSK (Differential Binary Phase-Shifi Keying), druhá DQPSK (Differential Quadrature Phase-Shifi Keying). Třetí úroveň přidává k DBPSK kvadraturní amplitudovou modulaci QAM (Quadrature Amplitude Modulation) a poslední úroveň 48 a 54 Mbit/s kombinuje DQPSK a QAM .

3.3.1.5.3 FHHS (Frequency Hopping Spread Spectrum)

(7) Původní myšlenkou při vývoji přeskokových zařízení bylo vytvořit systém, který umožní udržet radiově naváděná torpéda na správném kurzu a zabránit nepříteli v rušení naváděcího systému. Princip spočíval v tom, že pokud systém bude velmi rychle skákat z jednoho kmitočtu na druhý, může se tak vyhnout rušení, protože rušička nedokáže měnit vysílanou frekvenci stejně rychle jako vysílač. Tato myšlenka dala vzniknout technologii FHSS .
Standard 802.11 implementuje 79 kanálů, každý o šířce 1 MHz, čímž pokrývá celý rozsah od 2,4 do 2,483 GHz. Čas setrvání je 20 ms. Skokový obrazec je dán pseudonáhodným algoritmem, což znamená, že pokud tento skokový obrazec není znám, bude sekvence zpráv nesrozumitelná a s největší pravděpodobností také i nedetekovatelná.

3.3.2 Topologie bezdrátové sítě

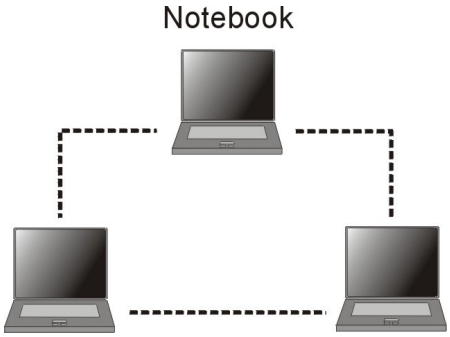
Termín topologie se používá pro označení základního uspořádání sítě. Jedná se především o fyzické uspořádání počítačů a dalších komponent v síti.

WiFi sítě lze nastavit dvěma základními způsoby:

- IBBS (Independent Basic Service Set) – klienti se připojují mezi sebou navzájem
- BSS/ESS (Basic Service Set / Extended Service Set) – klienti se připojují k centrálnímu přístupovému bodu

3.3.2.1 IBBS (Independent Basic Service Set), Ad-hoc sítě

(7,10) IBBS též označován jako režim ad-hoc. Pracuje v režimu peer-to-peer to znamená, že ke své činnosti nepotřebuje přístupový bod. Tento režim je vhodný zejména pro dočasné propojení počítačů nebo pro sítě, jež obsahují malý počet bezdrátových klientů.
Původně byl režim ad-hoc určen pro rozsáhlé sítě s neúplnou viditelností, kde by každý uzel fungoval jako klient a zároveň jako směrovač předávající pakety dalším uzlům v síti. Tato myšlenka se ale příliš neujala a sítě v režimu ad-hock se mnohem častěji používají jako dočasná náhrada rozbočovače (např. konference atp.). V tomto režimu stačí počítače pouze zapnout a propojit s kolegy. Nevýhodou tohoto řešení je slabá bezpečnost tohoto uspořádání.



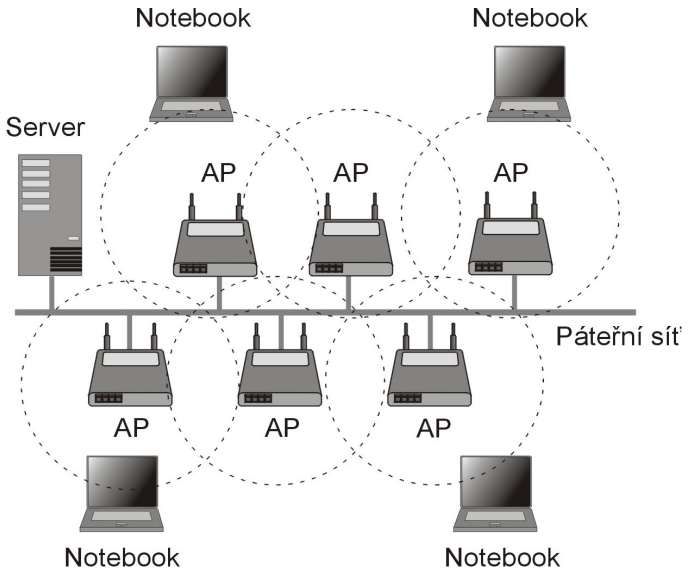
Obrázek 3.5 : Ad-hoc síť

3.3.2.2 BBS (Basic Service Set) / ESS (Extended Service Set), Infrastrukturní sítě

(1) **BSS** (Basic Service Set) je základní soubor služeb pro sítě sestávající se ze zařízení, která jsou všechna ve vzájemném dosahu nebo v dosahu jednoho přístupového bodu.

(1) **ESS** (Extended Service Set) sítě s rozšířeným souborem služeb umožňují překrývání většího počtu přístupových bodů, což značně rozšiřuje dosah jedné sítě.

(1) **BSS/ESS** přístupové body fungují v rámci ESS jako mosty mezi sítěmi BSS, které tvoří ESS, přičemž umožňují každé stanici v síti komunikovat s jakoukoliv jinou stanicí a dále umožňují mobilním stanicím pohyb mezi segmenty dané sítě. Všechny přístupové body musí být nastaveny jako členové jedné sítě (tj. mají stejný název sítě, stejné bezpečnostní nastavení atp.). Každý přístupový bod komunikuje na jiném kanálu z důvodů rušení mezi přístupovými body. Toto uspořádání umožňuje mobilní stanici, která se dostane mimo dosah svého přístupového bodu jeho nové automatické přidružení k jinému přístupovému bodu, který je v dosahu stanice. Při návrhu sítě je vhodné umístit jednotlivé přístupové body tak, aby se jejich oblasti pokrytí překrývaly, čímž se zabrání mezerám v přístupu pro pohybující se stanice.
Pro společnou práci přístupových bodů je nutné aby podporovaly protokol vzájemné komunikace přístupových bodů IAPP (Inter Access Point Protocol). Protokol zajišťuje, aby všechny přístupové body v ESS věděly o všech stanicích připojených k ostatním přístupovým bodům.



Obrázek 3.6: Infrastrukturní síť

3.4 Hardwarové vybavení bezdrátových sítí

3.4.1 Přístupový bod (Access point)

(10) Přístupový bod nebo také AP (Access Point) zajišťuje přístup bezdrátových zařízení k lokální síti, přístup na internet, most mezi bezdrátovými zařízeními a kabelovými sítěmi atd..
Většina přístupových bodů jsou malé skřínky s jednou či více anténami. Bez ohledu na design jsou všechny z hlediska své vnitřní struktury stejné. Každý přístupový bod obsahuje minimálně jeden radio přijímač/vysílač pracující na frekvenci podle norem 802.11, programové vybavení pro řízení přístupového bodu a bezdrátové sítě (firmware) a porty pro připojení přístupového bodu ke kabelové sítí (LAN port) a k internetu (WAN port). Další nezbytnou součástí přístupových bodů je anténa.

Obrázek 3.7: AP / WiFi Router (OVISLINK WL-1000R), AP / WiFi Router (Linksys WRT54GS r)

3.4.1.1 Radiostanice

(10) Každý přístupový bod obsahuje alespoň jednu radiostanici, která určuje, kterou normu bezdrátové komunikace dané zařízení podporuje. V současné době patří mezi nejrozšířenější norma 802.11b (11 Mbit/s). Někteří výrobci dodávají přístupové body bez radiostanic a nechávají na uživatelích, aby si přístupový bod radiostanicí dovybavili.

3.4.1.2 Komunikační porty

(10) Přístupové body zpravidla obsahují ethernetový WAN port pro širokopásmové připojení na internet ať už přes kabelový nebo DSL modem. Dále obsahují několik LAN portů k připojení lokální sítě. K LAN portům lze připojit rozbočovač (HUB), který může být také nahrazen přepínačem (Switch). LAN porty přístupových bodů jsou zpravidla přepínanými porty.

3.4.1.3 Antény

(10) Součástí přístupových bodů je jedna nebo dvě malé antény, které umožňují spolehlivou komunikaci zařízení v řádu několika desítek metrů. Většina přístupových bodů také obsahuje port pro připojení externí antény pro zvětšení dosahu. Připojením výkonné externí antény lze dosah WiFi sítě zvětšit na stovky metrů, v extrémních případech až na několik kilometrů.

3.4.1.4 Důležité vlastnosti přístupových bodů

- Administrace přístupu
- Firewall
- Šifrování WEP/WPA/802.11i
- DHCP/NAT

Bližší popis vlastností přístupových bodů je popsán v kapitolách 4 (Správa sítí) a 5 (Bezpečnost sítí).

3.4.2 Softwarový přístupový bod

Jedná se o počítač vybavený softwarem pro směřovaní (routování), obsahující jeden nebo více WiFi adapterů, ethernetový adaptér a zpravidla je vybavený také switchem pro připojení lokální sítě. Použít lze starší počítač, který bude tomuto účelu vyhovovat a vybavit ho vhodným operačním systémem (např. Linux). Dostáváme řešení, které oproti klasickým přístupovým bodům umožňuje mnohem širší uplatnění, ale vyžaduje hlubší znalosti správy počítačových sítí a znalost operačního systému Linux.

3.4.3 Síťový most

(1) Síťový most (bridge) slouží k spojení dvou segmentů sítě. Díky bezdrátovým mostům můžou dva segmenty LAN sítě pracovat jako jediná síť. Mnoho výrobců funkci síťového mostu integruje do svých přístupových bodů.

- Point to Point – Propojení dvou bodů, slouží k propojení dvou oddělených LAN sítí.

- Point to Multipoint – Propojení více bodů, slouží k propojení jedné sítě s více LAN sítěmi, v podstatě se jedná o rozšíření funkce Point to Point.

3.4.4 Bezdrátový opakovač (repeater)

(1) Bezdrátový opakovač přijímá bezdrátový signál od zdroje, provádí jeho zesílení a dále ho vysílá do cílového místa. Opakovače se používají v případech, kdy je potřeba rozšířit oblast pokrytí bezdrátové sítě.

3.4.5 WiFi Síťový adaptér

3.4.5.1 Součásti síťového adaptéru

Každý síťový adaptér obsahuje radiostanici a konektor který odpovídá jednomu I/O portu daného počítače. Často síťové adaptéry obsahují malou anténu pro zvýšení dosahu a nebo konektor pro připojení externí antény.

3.4.5.2 Druhy síťových adaptérů

3.4.5.2.1 PCMCIA karty

(10) Naprostá většina notebooků obsahuje jeden nebo více PCMCIA slotů pro PC karty Type II. Většina WiFi radiostanic jsou karty typu Type II slučitelné s Card Bus, což je 32bitová verze PCMCIA.
Výhody PCMCIA síťových adaptérů jsou v jejich snadné instalaci, kompaktních rozměrech, kompatibilitě a v neposlední řadě také v ceně těchto zařízení. Použití je implicitně pro notebooky a jiná přenositelná zařízení vybavená PCMCIA slotem.

3.4.5.2.2 PCI síťové adaptéry

(10) Jsou určeny především pro stolní PC, komunikace probíhá přes PCI sběrnici. Výhodou těchto zařízení je, že s nimi lze vybavit téměř jakýkoliv stolní počítač PC. Většina z nich má výstup pro externí anténu pomocí reverzního SMA konektoru a disponuje rozhraním PCI 2.1. Pouze nejnovější PCI karty standardu 802.11g jsou pouze pro sběrnici PCI 2.2. Nebudou tak fungovat ve starších počítačích. V dnešní době čím dál více výrobců integruje WiFi síťové adaptéry do základních desek. WiFi adaptér se tak stává standardním vybavením PC.

3.4.5.2.3 USB síťové adaptéry

(10) Jsou WiFi adaptéry, které se připojují k počítači přes USB sběrnici, kterým je vybaven každý stolní počítač i notebook. Díky tomu jsou USB adaptéry nejflexibilnějším druhem adaptéru, pomocí něhož se může počítač připojit do WiFi sítě. Nevýhodou USB adaptéů je, že v naprosté většině nejsou vybaveny žádným konektorem pro připojení externí antény. Své uplatnění USB adaptéry nacházejí při použití v kancelářském a domácím prostředí, kde je dobře dostupný signál bezdrátové sítě.

Obrázek 3.8: PCMCIA karta (OvisLink WL-8000PCM), PCI bezdrátová karta (OvisLink WL-8000PCI), USB WiFi klient (ASUS WL-167g)

3.4.6 Antény

(1) Základní funkcí antén je, že zvyšují dosah a pokrytí WiFi sítí. Jednou z nejdůležitějších věcí, které je nutné v souvislosti s anténami chápat je, že antény nezesilují signál. Slouží pouze k tomu, že vyzařovanou energii zaostřují do určitého směru.
Většina síťových adaptérů a přístupových bodů se dodává s malou anténou. Tyto vestavěné antény jsou velmi slabé. Někteří výrobci notebooku dodávají počítače s integrovanou anténou, která je uložena v těle notebooku nejčastěji uvnitř LCD displeje, což z části eliminuje nevýhody slabých antén dodávaných se síťovými adaptéry.
Většina přístupových bodů a síťových adaptérů podporuje připojení externí antény, která nahrazuje antény dodávané výrobci těchto zařízení jako součást balení. To umožňuje zvýšit dosah přístupových bodů až na několik kilometrů při vhodném umístění antény (např. na střeše).

3.4.6.1 (1) Charakteristické vlastnosti společné pro všechny typy antén

- 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.

3.4.6.2 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 jejího pokrytí a sílou signálů.

Obrázek 3.9: Všesměrová anténa (OvisLink WAE-085GP), Směrová anténa typu Yagi (OEM YAGI16), Směrová parabolická anténa (OEM UNI24)

3.4.6.2.1 Všesměrové antény

(1) Jak už název těchto antén napovídá 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.

3.4.6.2.2 Sektorové antény

(1) Jsou obdobou všesměrových antén. Narozdíl od nich je jejich úhel vyzařování maximálně 180 stupňů. Jelikož jsou sektorové antény směrovější, dosahují také většího zisku a jsou méně citlivé na šum než všesměrové antény. Sektorové antény jsou vhodné tam, kde všechna zařízení leží v jednom směru.

3.4.6.2.3 Yagi antény

(1) Jsou primárně určeny pro propojení přístupových bodů na delší vzdálenosti. Jsou to směrové antény s úhlem vyzařování 15-60 stupňů a poskytují vyšší zisk než sektorové antény.

3.4.6.2.4 Panelové antény

(1) Jsou ploché antény s pevnou konstrukcí. Podobně jako ostatní směrové antény jsou i tyto vysoce směrové a hodí se k propojení dvou přístupových bodů.

3.4.6.2.5 Parabolické antény

(1) Mohou být jak kulatého tak obdélníkového tvaru. Jsou vhodné pro venkovní instalaci. Mohou být tvořeny mřížkou nebo pevnou konstrukcí. Dosahují největších zisků a jsou vysoce směrové a proto se hodí k venkovnímu propojení dvou přístupových bodů na delší vzdálenosti.

3.4.6.2.6 Antény typu „HomeMade“

(1) Mnoho uživatelů a to především z řad radioamatérů, dává přednost výrobě antény před její koupí. Sestavení vlastní antény však vyžaduje specifické znalosti výpočtů pro dosažení správné frekvence a zisku. Dále je nutné dodržet předpisy dané generální licencí GL–12/R/200 stanovenou ČTÚ týkající se úrovně zesílení signálu, která je v daném pásmu přípustná.
Na internetu je mnoho stránek věnujících se problematice tvorby vlastní WiFi antény s podrobným popisem a návodem na jejich výstavbu. Mnohdy tyto podomácku vyrobené antény dosahují solidních parametrů a mohou být alternativou k běžně dostupným komerčním anténám.

3.4.7 Konektory a kabelová vedení

(9) Kabely se ve WiFi sítích používají k propojení antény s přístupovým bodem nebo síťovým adaptérem. Používají se koaxiální kabely určené pro práci v pásmu 2,4 GHz.
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 m) je vhodné použít tenké kabely s průměrem 5 mm, jejich útlum se pohybuje okolo 0,5 dB/m. Jsou tenké a dobře tvarovatelné, další jejich výhodou je široká dostupnost konektorů (např. RSMA konektory, TNC, SMA atd.).
Pro delší vzdálenosti a při venkovním 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 možnou cestou, bez prudkých ohybů, kroucení a smyček. Kabel se nesmí namotávat na žádné kovové trubky ani stožáry a nesmí se ani vést uvnitř těchto stožárů, nepožívají se kovové průchodky.
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.
Konektory typu SMA se používají v aktivních prvcích a nejsou určeny pro venkovní použití. Jejich útlum se pohybuje 0,1-0,5 dB pro pár konektorů. Nevýhodou je jejich dostupnost pro silné koaxiální kabely (11mm), v takovém případě je vhodné použít konektor typu TNC.
Nejrozšířenějším typem konektoru je konektor typu N. Je velice robustní a používá se pro venkovní instalace. Útlum těchto konektoru se pohybuje kolem 1 dB/m.

4 Správa sítí

4.1 Správa a konfigurace přístupového bodu

Přístupový bod umožňuje správu a konfiguraci sítě pomocí jeho konfiguračního softwaru.

4.1.1 (9) Možnosti konfigurace přístupových bodů

- Klientský software – Používá se zpravidla pro platformu Windows, bývá zpracován formou tzv. „wizardů“, neboli průvodců, kteří provedou uživatele kompletní instalací krok za krokem.

- SNMP (Simple Network Management Protocol) – Označuje síťový protokol a standard zpřístupňující dohodnuté postupy, pravidla a architekturu pro management sítě TCP/IP nebo IPX a jejich síťových prvků. Vyžaduje základní znalosti terminologie a je méně uživatelsky přátelský oproti klientskému softwaru.

- Webové rozhraní – Patří mezi nejrozšířenější způsoby konfigurace přístupových bodů. Webový prohlížeč, který je standardní součástí každého operačního systému, umožňuje snadnou konfiguraci a správu přístupového bodu.

- Telnet – Správu přes telnet ocení uživatelé, kteří vyžadují dálkovou správu po vytáčené lince.

4.1.2 (9,10)Přístup na internet

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

- Automatické získání IP Adresy. Přístupový bod si vyžádá od serveru IP adresu a tu si ponechá dokud se neodpojí od internetu.

- Statická IP adresa. ISP (Internet Service Provider) Vám přidělí permanentní veřejnou IP adresu.

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

- PPTP (Point-to-Point Tunnelling Protocol) bod-bod tunel protokol používá se pro připojení k ADSL lince.

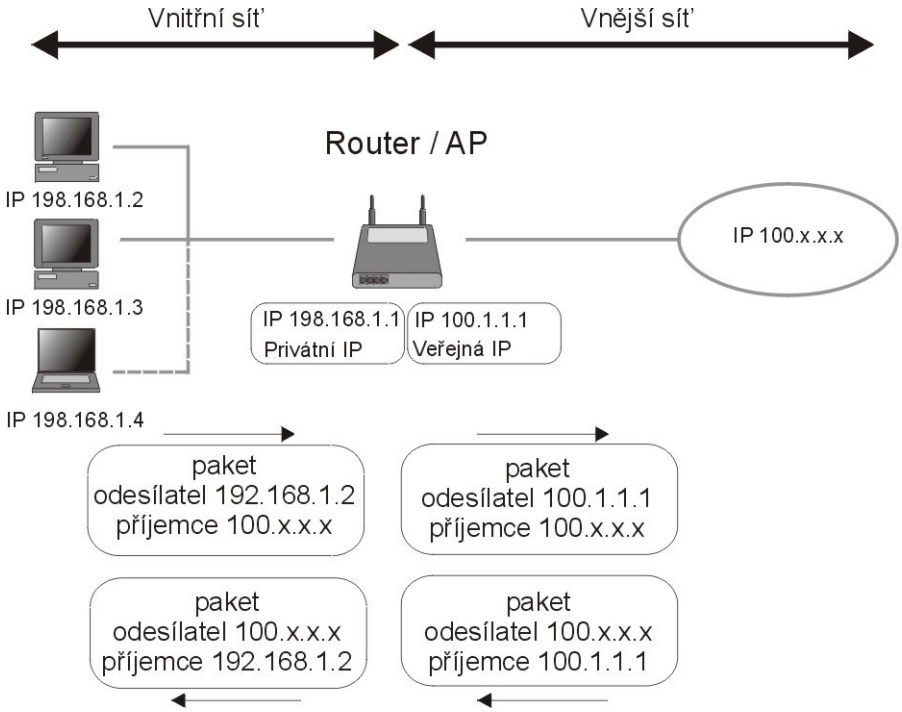
- DHCP (Dynamic Host Configuration Protocol) klient podpory dynamické konfigurace znamená, že přístupový bod může získat IP adresu pro sebe od ISP namísto použití statické adresy.

4.1.3 DHCP server

(10) DHCP server poskytuje počítačům připojeným ať už bezdrátově nebo kabelem přístup na síť přes TCP/IP protokol. Každému počítači na síti přiřazuje IP adresu, která slouží k jeho identifikaci. IP adresy přiděluje dynamicky (při každém připojení počítače do sítě) a nebo staticky (permanentně přidělená IP adresa). V kombinaci s překladem síťových adres NAT (Network Address Translation), který umožňuje, aby několik počítačů sdílelo jednu veřejnou IP adresu. Všechny počítače připojené do sítě tak mohou využívat jednu veřejnou IP adresu přiřazenou od ISP.
DHCP server je standardním vybavením přístupových bodů, a většina jich obsahuje i NAT.

4.1.4 Veřejné a privátní IP adresy

(10) Veřejné IP adresy přiděluje ISP a slouží k jednoznačné identifikaci na internetu (vnější síť). Privátní IP adresy se používají k identifikaci počítače v lokální síti (vnitřní síť) a nejsou na internetu rozpoznávány. Pokud chceme sdílet připojení k internetu, musíme za jednu veřejnou IP adresu, kterou obdržíme od ISP schovat lokální síť. Ke 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 .



Obrázek 4.10: Směrování síťové komunikace, NAT

4.1.5 Firewall

(10) Firewall chrání počítač před vnějším napadením a nežádoucím průnikům do sítě z internetu. Tuto činnost 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 pro svoji komunikaci má přiřazena čísla portů, které používá pro svojí komunikaci. Každý port je očíslován (např. webový prohlížeč používá port 80, FTP (File Transfer Protocol) používá port 21 atd.).
Jestliže je port na počítači otevřen může s ním navázat komunikaci kdokoliv, kdo zná IP adresu daného počítače. Buď prostřednictvím aplikace k tomuto účelu určené (např. v případě portu 80 to je webový prohlížeč) 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 počítače před nežádoucími návštěvníky. Také umožňuje nastavit přístup na určité porty 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 tohoto firewallu proti průnikům z internetu, ale komunikace na úrovni lokální sítě (vnitřní síť) probíhá bez omezení.
Firewall přístupového bodů neobsahuje tolik funkcí jako softwarový firewall. Softwarový firewall nabízí mnoho dalších doplňkových služeb a funkcí (např.

povolování komunikace jen některým aplikacím, nastavení filtrování na základě klíčových slov, ochrana proti spywaru, omezení služeb, omezení přístupu ke specifickým serverům a mnoho dalších služeb). Je proto vhodné nespoléhat se jen na firewall přístupového bodu a lze proto doporučit instalaci softwarového firewallu na všech počítačích v síti.

4.1.6 DMZ – demilitarizovaná zóna

(10) Demilitarizovaná zóna umožňuje, aby počítač ve vnitřní síti byl 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 e-mailových serverů. Většina přístupových bodů podporuje pouze jeden počítač v DMZ.

4.1.7 Přesměrování portů

(10) 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 specifických portů, které budou k dispozici pro vnější síť (internet), zatímco zbývající část vnitřní sítě zůstane chráněna. Počítač, na který je provoz přesměrován, musí mít nastavenou statickou IP adresu. Přesměrování portu využívají například on-line hry, IP telefonie, P2P klienti a mnoho dalších podobných aplikací.

4.1.8 Filtrování

(10) Řada přístupových bodů nabízí možnost filtrování služeb a přístupu na internet. Filtry umožňují blokování určitých serverů, omezení přístupu na základě klíčových slov nebo zdrojové domény, omezit přístup na internet v určitých hodinách a také na určité porty.

4.1.9 VPN (Virtual Private Network)

(8,10) VPN umožňuje počítačům připojeným k internetu bezpečně přistupovat k prostředkům privátní (vnitřní) sítě. K privátní síti přistupují počítače prostřednictvím nedůvěryhodné transportní sítě nejčastěji internetu, přičemž dochází k šifrování všech dat přenášených ze vzdáleného počítače na privátní síť. Tato služba umožňuje, aby například zaměstnanci využívali privátní firemní síť, když se nacházejí mimo kancelář.
VPN zajišťuje větší bezpečnost přenášených dat než bezpečnostní mechanizmy normy 802.11. Existuje celá řada protokolů VPN mezi nejpoužívanější patří protokoly PPTP a L2TP, především z důvodu podpory operačního systému Windows. Je nutné si ověřit u správce VPN sítě, jaký druh přístupu podporuje.

5 Bezpečnost sítí

Bezdrátová síť má oproti kabelovým sítím jednu bezpečnostní nevýhodu, vycházející z principu komunikace těchto sítí. Na rozdíl od kabelových sítí na to, aby někdo mohl odposlouchávat komunikaci v bezdrátové síti stačí, aby zachytil 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 neoprávněným přístupům

5.1 Šifrování

5.1.1 WEP (Wired Equivalent Privacy)

(7,8) 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).
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 s 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 ní vypočítá kontrolní součet a porovná se s přijatým součtem. Pokud oba součty souhlasí, zpráva je v pořádku.
Hlavní chybou v návrhu protokolu WEP je, že není specifikováno, jak se má generovat inicializační vektor. Inicializační vektor je 24 bitová 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). Odesilatel i příjemce musí znát hodnotu tohoto klíče. Problém je v tom, že protokol 802.11 neřeší správu tohoto klíče a jeho distribuci mezi uživatele. 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.
WEP definuje délku klíče 40 bitů, před těchto 40bitů 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 však není přesný, protože 24 bitů tohoto klíče je inicializační vektor, který se přenáší nešifrovaný. To znamená, že délka klíče je pouze 40 nebo 104 bitů.
I přestože protokol WEP má 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

(9) 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.

802.11 specifikuje dvě metody pro autentizaci:

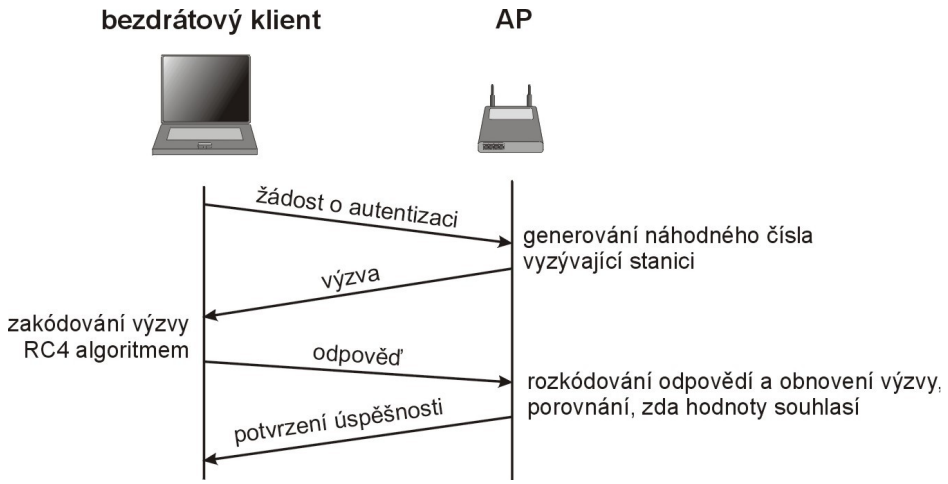
- Open-system autentizace
- Shared-key autentizace

5.2.1 Open-system autentizace

(9) 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 přistup do sítě.

5.2.2 Shared-key autentizace

(9) 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 také schopno užívat autentizaci se sdíleným klíčem.



Obrázek 5.11: Autorizace Sdíleným klíčem (shared-key)

5.2.3 Filtrování adres

(9) 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 jiné varianty založené na autentizaci pomocí MAC adres. Například lze vytvořit seznam MAC adres, kterým je naopak přístup do sítě zakázán, omezit přístup časově a nebo umožnit používat jen určitou šířku pásma atp..
Problém autentizace pomocí filtrace MAC adres je, že MAC adresa jako jednoznačný identifikátor je uložena 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 přistup do sítě povolen než si náhodně upravit MAC adresu, která má přístup do sítě zakázán.

5.2.4 802.1x, EAP (Extensible Authentication Protocol)

802.1x je založen na protokolu EAP, jedná se o mechanizmus přenosu EAP paketů prostřednictvím spojové vrstvy LAN (typu 802). Zprávy EAP se zapouzdřují do rámců 802.1x.

Jeho tři základní komponenty jsou :

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

(8) Aby mohl protokol řádně fungovat je nutné, aby byl jak protokol 802.1x tak zvolený EAP konzistentně podporován ve všech třech 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 slouží pouze ke komunikaci autentizátora s autentizačním serverem. Řízený 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.

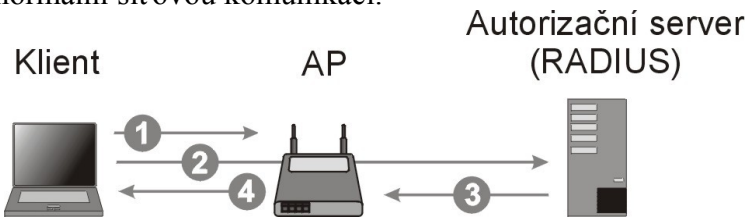
(8) **Autentizace podle 802.1x je znázorněna na obr. 5.2**

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

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

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

4. 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 5.12: Autentizace podle 802.11x

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

5.3 WPA (WiFi Protected Access)

(8) 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 (Tempoval Key Integrity Protocol) a řízení přístupu (802.1x).
TKIP využívá stejného algoritmu šifrování jako WEP, používá standardně 128 bitový klíč a dočasné 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.
WPA představuje řešení všech známých problémů protokolu WEP.

5.4 IEEE 802.11i

(8) 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.
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 také 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.
CCPM obsahuje algoritmus MIC, zajištující ověření, že nedošlo k modifikaci přenášených dat. Výpočet MIC je založen na hlavičkových hodnotách vycházející z inicializačního vektoru a z dalších hlavičkových informací ve 128 bitových 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.

5.5 Základní kroky k zabezpečení Wifi sítě

- Aktualizace firmware – Pravidelnou aktualizací firmwaru lze odstranit řadu bezpečnostních problémů. Firmware lze stáhnout z domovských stránek výrobce přístupového bodu.

- WEP/WPA/ IEE802.11i – Aktivujte WEP šifrování. Pokud je to možné přejděte na WPA nebo novou bezpečnostní normu IEEE 802.11i.

- SSID – Zrušte vysílání SSID, mnoho přístupových bodů umožňuje vypnout SSID broadcast, tím se docílí toho, že většina WiFi zařízení síť neuvidí.

- Filtrace MAC adres – Filtrace MAC adres je poměrně dobrá metoda k zvýšení zabezpečení sítě, doporučuje se vytvořit seznam MAC adres s povoleným přístupem než naopak.

- Firewall – Pomocí firewallu oddělte přístup z vnitřní sítě do internetu

- VPN – Pokud je to možné, používejte přístupové body s podporou IPSec, které mohou zajišťovat bezpečný tunel mezi přístupovým bodem a koncovým uživatelem.

- Access point – Zajistěte přístup k administraci přístupového bodu heslem a často toto heslo měňte.

6 Návrh a správa konkrétní sítě

Při plánování a návrhu metropolitní WiFi sítě INET jsme si ujasnily hlavní kroky budování budoucí bezdrátové sítě.

- Propustnost sítě – Požadavky na propustnost sítě patřily mezi základní.Pro využití maximální propustností pátěřní sítě jsme využily zařízení podporující normu 802.11a. Koncové přístupové body AP byly naplánovaly na starší normě 802.11b.

- Oblast pokrytí – Požadavky na pokrytí jsou důležité při plánování této WiFi sítě.Byla navržena orientační mapa se zakreslením rozmístění přístupových bodů a oblast jejich pokrytí.

- Mobilita – U této WiFi sítě,vzhledem k rozlehlosti nebylo možné zajistit mobilitu,protože jednotlivé AP se svým signálem nepřekrývají.

- Uživatelé – Počet uživatelů a jejich nároky na používaní sítě byl 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 – Byla navržena hierarchie přidělování IP adres uživatelům podle lokalit sítě.Nastavili jsme směrování provozu a rozhodli zda bude vhodné používat nebo nepoužívat DHCP server,případně s jakým nastavením.

- Bezpečnost – Bylo bráno v úvahu zabezpečení sítě, především pak autentizace přihlášení klientských stanic pomocí šifrování WEP.Naplánovali jsme uzavřenou síť s uzavřeným přístupem do ní.Přístup k internetu je zabezpečen pomocí povolení MAC adres .

- Vliv prostředí – Posouďili jsme vliv prostředí na fungování bezdrátové sítě a zjistily zda signál nebude muset procházet přes nějaké překážky nebo jsou-li přístupové body v přímé viditelnosti atp.. Zjistily a proměřily si ostatní WiFi sítě v dané lokalitě,abychom se vyhnuli vzájemnému rušení s ostatními bezdrátovými sítěmi.

6.1 Konfigurace přístupového bodu

Obrázek 6.13: Přístupový bod / Router Asus VL530g

Pro praktickou ukázku konfigurace přístupového bodu byl vybrán přístupový bod Asus VL530g. Tento přístupový bod patří mezi nejlépe vybavené přístupové body na trhu, obsahuje všechny standardní funkce většiny současných přístupových bodů a nabízí i řadu funkcí, které nejsou u současných přístupových bodů standardem.

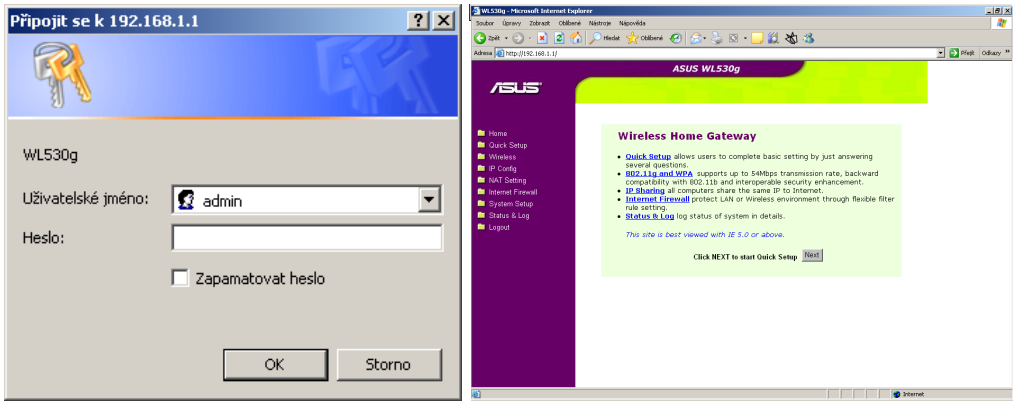
WAN port	RJ 45 10/100 BaseT
LAN port	4x RJ45 10/100 BaseT
Protokoly	TCP/IP, DHCP server a Klient, PPPoE, PPTP, NAT, ICMP, UDP,
Management	Vzdálená administrace, firmware restore, vyhledání zařízení (pomocí utility), save/restore, update přes web management
Frekvence	2.4 - 2.5 GHz
Přenosové rychlosti	802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps
	802.11b: 1, 2, 5.5, 11Mbps
Bezpečnost	64/128-bit WEP, WPA-PSK , TKIP,
	po upgrade firmwaru WPA-PSK2
Dosah	Uvnitř 40 m, venku (přímý výhled) 100 m at 11Mbps
	Uvnitř 25 m, venku (přímý výhled) 60 m at 54Mbps
Vysílací výkon	12 ~ 15 dBm
Napájení	AC přívod 100V - 240V (50 - 60 Hz), DC vývod 5V 2A
Velikost	129mm(Délka) 44mm(Šířka) 29mm(Výška)

Základní parametry přístupového bodu Asus VL530g

Přístupový bod Asus VL530g se konfiguruje přes webové rozhraní. Jeho webové rozhraní je podobné jako u jiných přístupových bodů a lze tedy předpokládat, že při konfiguraci jiných přístupových bodu lze vyjít z popisu konfigurace přístupového bodu ASUS VL530g. Řada funkcí a nastavení bude stejná či podobná nebo jinak sdružená a lze také předpokládat, že ne všechny funkce přístupového bodu Asus budou dostupné u jiných zařízení.

6.1.1 Základní nastavení

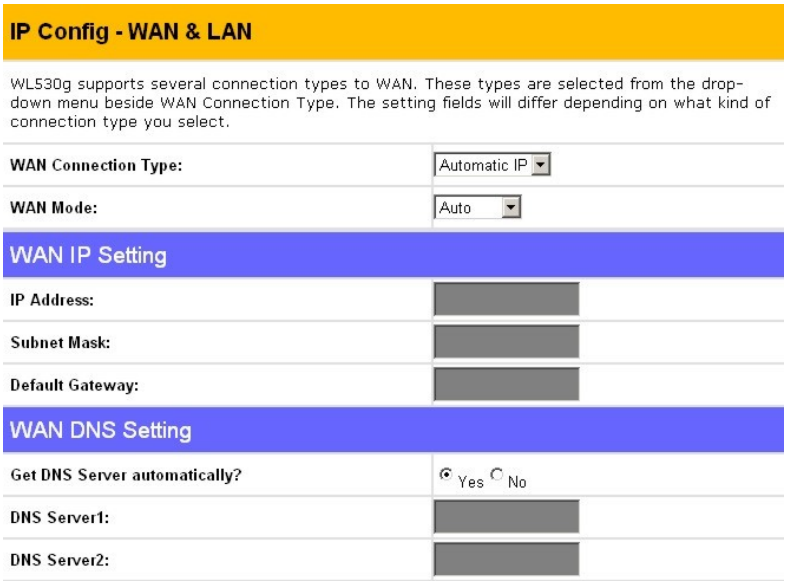
- Připojte přístupový bod k vaší síti, dále můžete připojit WAN konektor širokopásmového připojení k internetu. Připravte si informace o konfiguraci připojení k internetu od vašeho ISP.
- Do internetového prohlížeče zadejte IP adresu přístupového bodu, tovární IP adresa je 192.168.1.1 (bližší informace lze zjistit v technické dokumentaci přístupového bodu).
- Zadejte uživatelské jméno a heslo (tovární nastavení je zpravidla pro obě možnosti "admin", bližší informace lze zjistit v technické dokumentaci přístupového bodu).



Obrázek 6.14: Autentizace pomocí uživatelského jména a hesla, úvodní obrazovka webového rozhraní konfigurace přístupového bodu Asus VL530g

6.1.1.1 Nastavení WAN rozhraní

IP Config – WAN & LAN



Obrázek 6.15: Konfigurace WAN rozhraní

WAN Connection type
Slouží k výběru typu připojení do WAN sítě, k dispozici jsou tyto možnosti:

- *Statická IP* – Tuto možnost použijte, když Vám poskytovatel přidělí pevnou IP adresu.
- *PPPoE* - Někteří poskytovatelé vyžadují použit PPPoE pro připojení k jejich službám. Kontaktujte svého ISP pro více informací.
- *PPTP* – Jestliže používáte vytáčenou linku a adaptér VPN, tak musíte použít připojení pomocí PPTP.
- *Automatic IP* - Tuto možnost zvolte, pokud ISP přiděluje IP adresy automaticky.
- *Big Pond* – Služba vzdáleného přístupu v ČR se nepoužívá.

WAN mode
Umožňuje nastavit přístupový bod pro práci ve třech režimech:

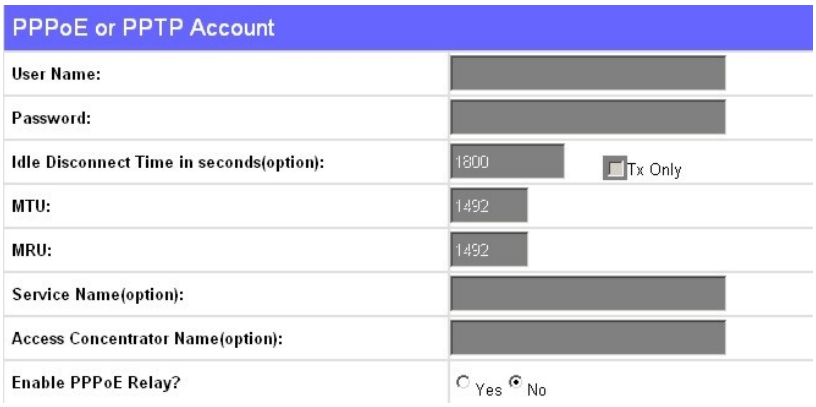
- *DISABLED* AP+5 portový switch
- *ENABLED* Router+4 portový switch
- *AUTO* Automaticky režim (AUTO)

WAN IP Setting
Slouží pro konfiguraci připojení k WAN sítí typu: Statická IP, PPTP

IP Address, Subnet Mask, Default Getaway: Nastavení IP adresy, masky a brány vzdálené sítě, pokud zůstane nevyp7lněné, AP se pokusí získat tyto údaje z DHCP serveru.

WAN DNS Setting
Get DNS Server automatically: Umožňuje automatické nebo ruční nastavení DNS serveru, poskytnutého ISP.

DNS Server 1,2: Pokud to váš ISP vyžaduje, zadejte do těchto polí IP adresy DNS serverů.



Obrázek 6.16: Konfigurace WAN rozhraní

PPoE or PPTP Account
Konfigurace připojení k vytáčenému připojení k internetu (PPoE nebo PPTP)

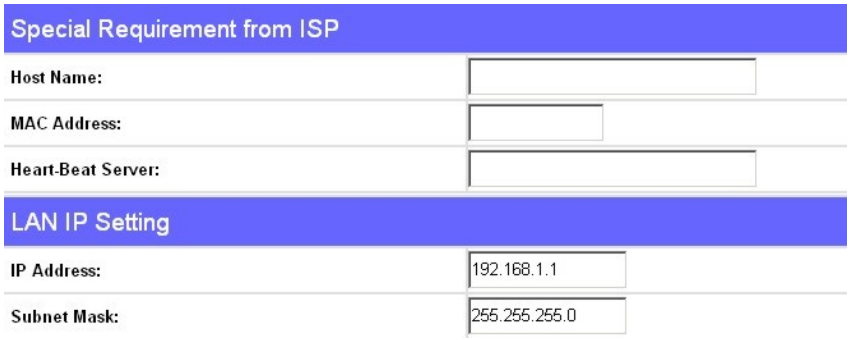
User Name / Password: Uživatelské jméno a heslo poskytnuté vašim ISP.

Idle Disconnect Time in seconds(option): Doba nečinnosti, po které je automaticky provedeno odpojení AP od internetu.

MTU (Maximum Transmission Unit): Nastavuje maximální velikost paketu přenášeného do internetu.

MRU (Maximum Transmission Unit): Nastavuje maximální velikost paketu přenášeného z internetu.

Enable PPoE Relay ?: Umožňuje klientským počítačům v LAN síti navázat vytáčené připojení prostřednictvím AP.



Obrázek 6.17: Konfigurace WAN rozhraní

Special Requirement from ISP

Host Name, MAC Address: Pokud vyžaduje ISP, tak vyplňte.

Heart-Beat Server: Pokud se připojujete přes Big Pond, tak se zadá IP Adresa serveru.

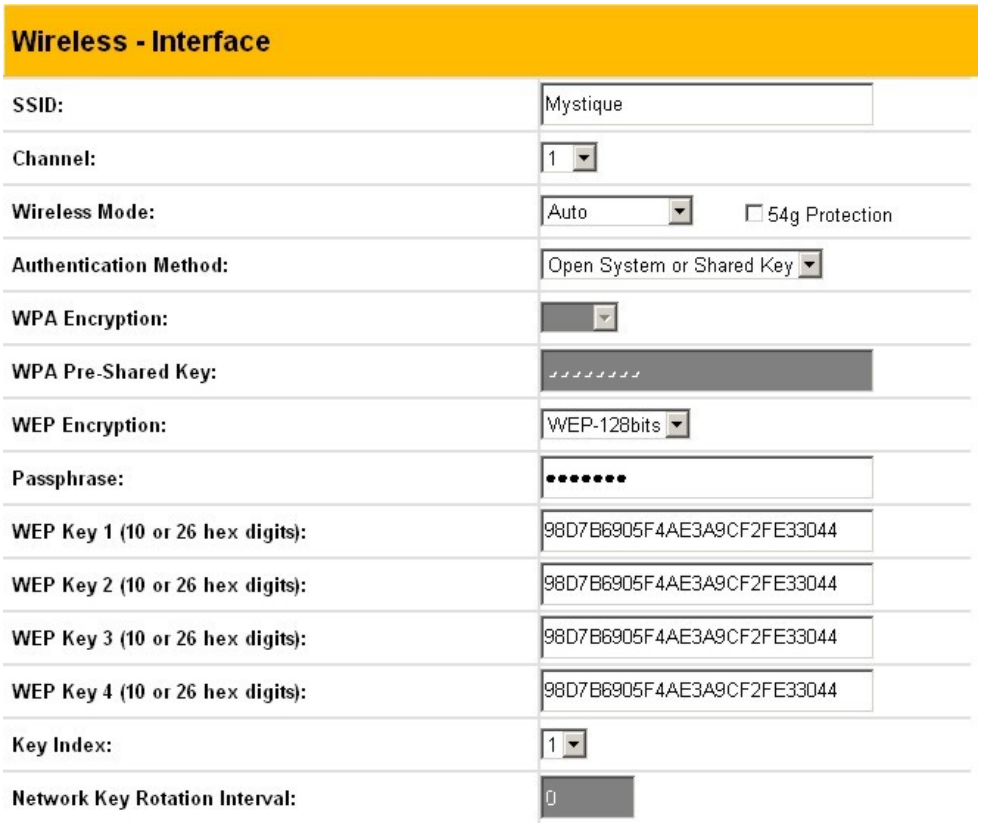
LAN IP Setting

IP Address: Nastavení IP adresy AP, kvůli bezpečnosti se doporučuje změnit na jinou IP adresu vyhrazenou intranetovým sítím. Tovární nastavení je v tomto případě 192.162.1.1.

Subnet Mask: Síťová maska určuje, kolik je možno připojit počítačů k LAN síti, tovární nastavení je 255.255.255.0 a není potřeba je měnit.

6.1.1.2 Nastavení bezdrátového rozhraní

Wireless Interface



Obrázek 6.18: Nastavení bezdrátového rozhraní

SSID: Zde nastavte název přístupového bodu. Tento název uvidí ostatní bezdrátová zařízení. V současné době se často jako SSID používá webová adresa dané WiFi sítě.

Channel: Nastavení kanálu radiové komunikace, v případě ESS sítě je nutné, aby každý AP v síti mělo jiný kanál a nedocházelo tak k interferencím. Je také vhodné si zjistit aktivní sítě v okolí daného AP a nastavit kanál takový, aby nedocházelo k rušení s těmito sítěmi.

Wireless Mode: Umožňuje nastavit komunikaci AP v normě 802.11b nebo 802.11g.

Authentication Metod: Výběr autentizační metody přístupového bodu, pokud všichni klienti podporují WPA, nastavte WPA-PSK pro lepší bezpečnost.

WPA: Pokud je zapnutá podpora WPA, umožňuje nastavit TKIP (Temporal Key Integrity Protokol)

WPA Pre-Shared Key: Zde nastavte heslo šifrováni WPA protokolu. Vyžadováno je 8-64 znaků.

WEP Encryption: Umožňuje nastavit velikost WEP klíče, buď 64 bitový nebo 128 bitový.

Passphrase: Na základě tohoto pole, se vygenerují 4 WEP klíče.

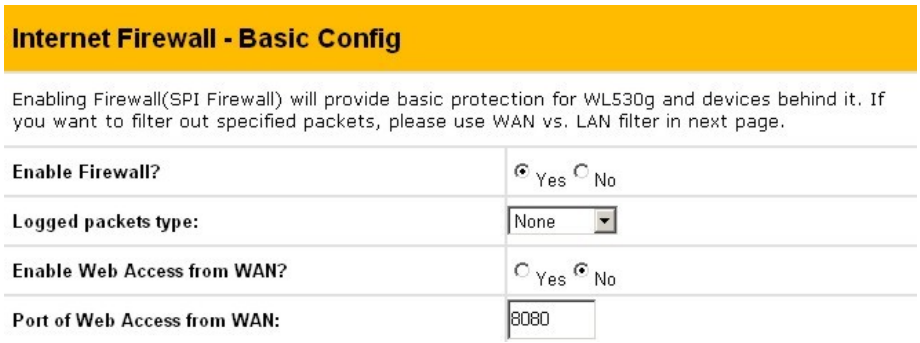
WEP key 1-4: V těchto polích se vygenerují WEP klíče, je možné je zadat také ručně, 64 bitový klíč má deset hexadecimálních číslic a 128 bitový klíč 26 číslic.

Key Index: Nastavuje jeden z čtyř WEP klíčů jako výchozí.

Network Rotation Key Interval: Udává čas rotace s jakou budou měněny WEP klíče, pokud nastavíte 0, nebude rotace WEP klíčů podporována.

6.1.1.3 Bezpečnost

Internet Firewall – Basic Config



Obrázek 6.19: Nastavení Firewallu

Enable Firewall?: Volba *Yes* zapíná firewall.

Logged packet typ: Toto pole zobrazuje, jaký druh paketů přenášených mezi sítí WAN a LAN bude logován.

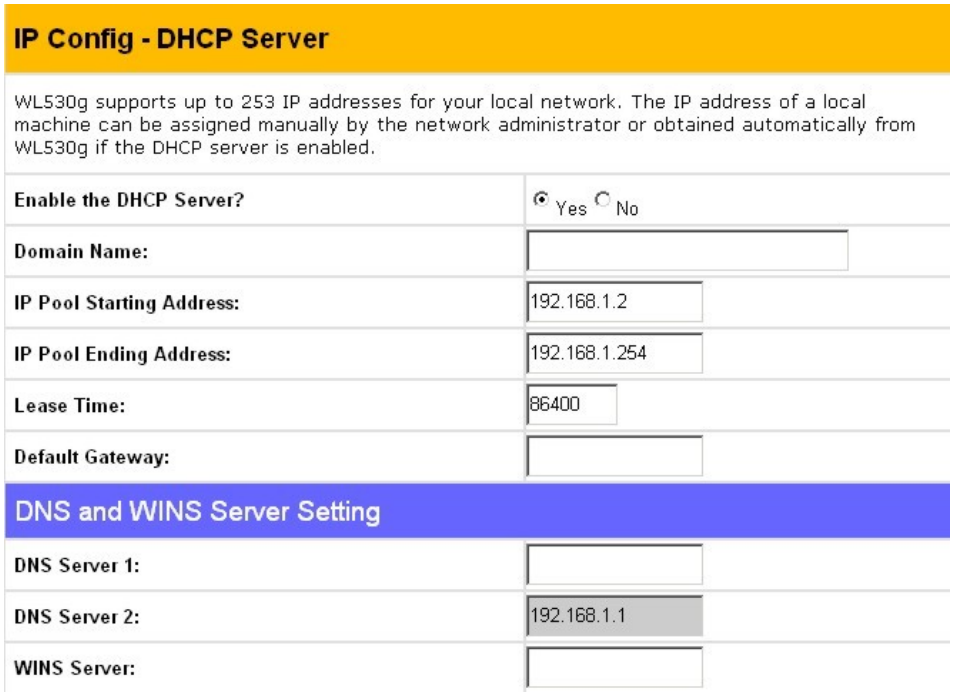
Enable Web Access from WAN?: Volba *Yes* povoluje webovou konfiguraci AP z internetu. Volba *No* umožní AP konfigurovat pouze z počítače připojeného do vnitřní sítě. Přístup ke konfiguraci AP přes internet představuje bezpečnostní riziko a proto pokud není nutné, pak je vhodné tento přístup ke konfiguraci AP zakázat.

Port of Web Access from WAN: Číslo portu, který bude použit v případě konfigurace AP z internetu. Z bezpečnostních důvodů je vhodné tento port zvolit z rozsahu 30000-65535.

6.1.2 Pokročilá nastavení

6.1.2.1 Nastavení WAN rozhraní

IP Config – DHCP Server



Obrázek 6.20: Nastavení DHCP serveru

Enable the DHCP Server?: Volba *Yes* zapíná DHCP server

Domain Name: Poskytuje klientům DHCP serveru doménové jméno serveru při žádosti o IP adresu DHCP serveru.

IP Pool Starting/ Ending Address: Určuje startovní/konečnou IP adresu, kterou bude DHCP server přiřazovat klientům.

Lease Time: Určuje dobu platnosti IP adresy, kterou poskytne klientům DHCP server. Pokud nebudete často měnit konfiguraci sítě, není nutné měnit tovární nastavení.

DNS and WINS Server Server

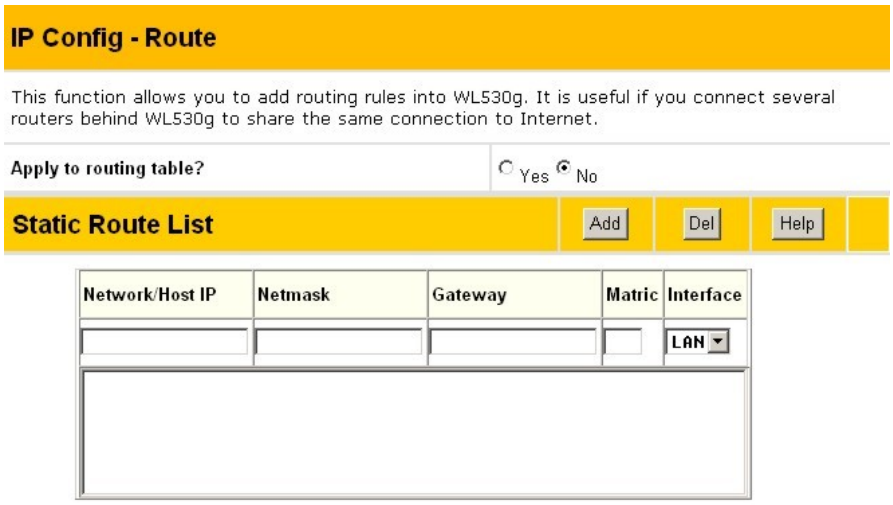
DNS Server 1,2: Slouží k ručnímu nastavení DNS serveru v případě, že je ISP nedoporučuje v konfiguraci DHCP nebo pokud chcete používat jiné servery.

WINS Server: Pokud používáte WINS (Windows Internet Naming Service), tak zadejte adresu WINS, jinak nechte pole prázdné.

Obrázek 6.21: Nastavení DHCP serveru

Assign IP Address Manually: Volba *Yes* povolí ruční přidělení statické IP adresy klientům vnitřní sítě LAN, na základě jejich MAC adresy.

IP Config - Route



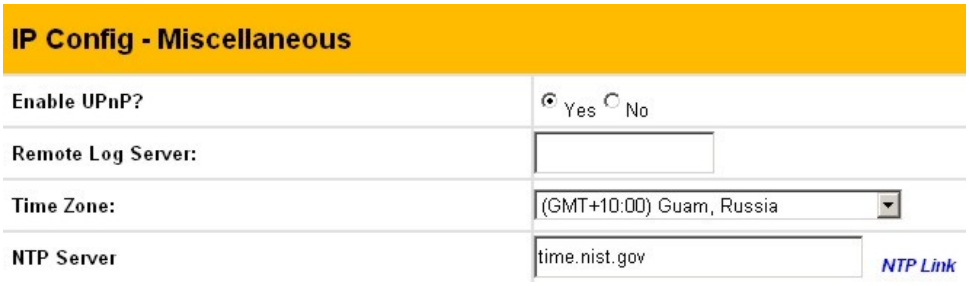
Obrázek 6.22: Konfigurace směrování

Apply to routing table?: Volba *Yes* povolí nastavení statického směrování (routing).

Static Route List

Statické směrování stanoví pevnou cestu, a to obvykle na vzdálenou síť. Nastavením voleb statického směrování *Network/Host IP, Netmask, Gateway* provedete nastavení datové cesty. Volba *Matric* umožňuje nastavit vzdálenost mezi sítěmi a tím rozhodnout o prioritě mezi cestami. Volba *Interface* nastaví rozhraní vzdálené sítě.

IP Config – Miscellaneous



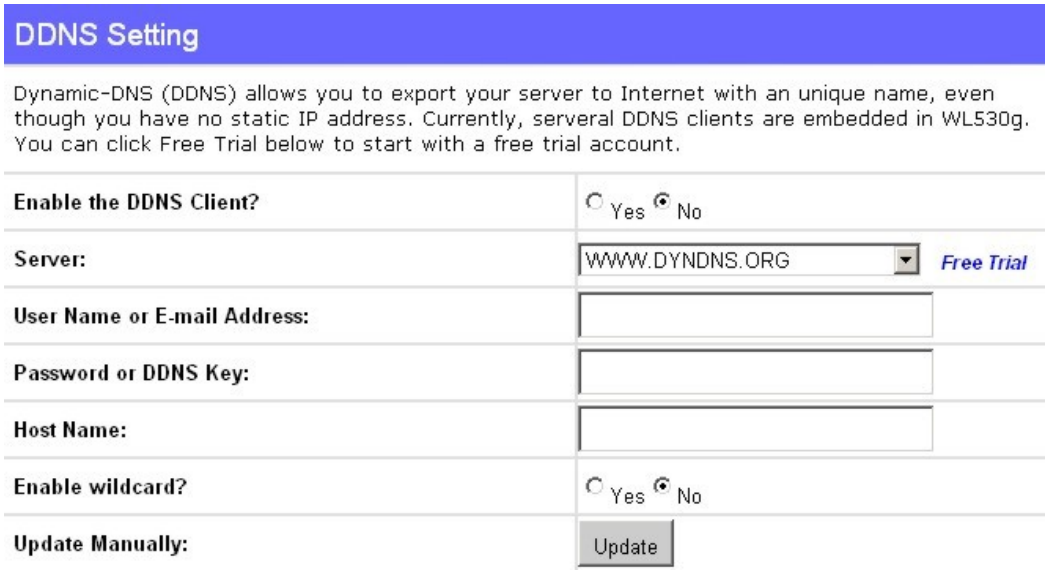
Obrázek 6.23: Doplňková konfigurace

Enable UPnP?: Volba *Yes* povolí univerzální systém Microsoft UPnP (Universal Plug and Play) který zajistí automatickou konfiguraci směrováni pro internetové aplikace a hry.

Remote Log Server: Umožňuje nastavit vzdálený server, který zaznamenává přihlašovací zprávy přístupového bodu, pokud pole zůstane nevyplněné zaznamená se 1024 zpráv.

Time Zone: Nastavení časové zóny.

NTP Server: NTP Server umožňuje synchronizovat systémový čas přístupového bodu.



Obrázek 6.24: Konfigurace dynamického DNS

DDNS Setting

DDNS nebo také dynamický DNS přiděluje počítači s dynamickou IP adresou doménové jméno. Tato služba aktualizuje záznam v databázi DDNS, podle toho, jakou IP adresu používáte. Pro použití této služby je nutné se registrovat na webových stránkách serveru, které poskytují tuto službu (AP Asus VL530g podporuje DynDNS.org, TZO.com). Služby vám přidělí doménu třetího řádu, která odkazuje na IP adresu vašeho AP. Na této adrese je pak možné zprovoznit například webový či FTP server, který bude pod touto adresou dostupný.

Enable DDNS Client: Volba *Yes* zapíná podporu DDNS klienta, který pokaždé, když dojde ke změně vaší IP adresy, aktualizuje záznam v databázi DNS.

User name or E-mail Address: Pole slouží k vaší identifikaci serverem zajištující službu DDNS

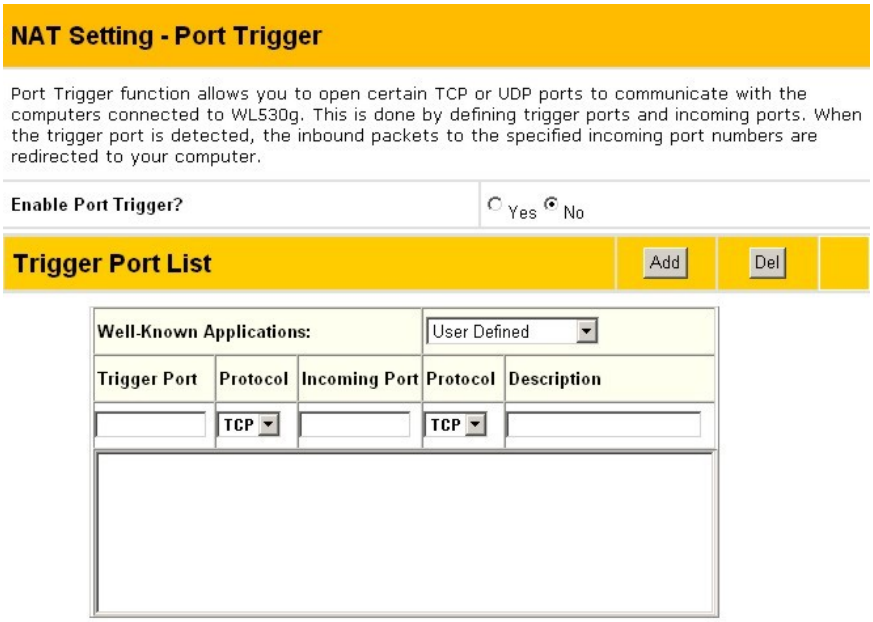
Password or DDNS Key: Pole slouží k vaší identifikaci serverem zajištující službu DDNS

Host Name: Doménové jméno ke kterému DDNS server přiřazuje vaší dynamickou IP adresu.

Update Manually: Umožňuje ruční aktualizaci DDNS databáze, například v případě výpadku DDNS serveru.

6.1.2.2 Nastavení Směrování

NAT Setting – Port Trigger



Obrázek 6.25: Konfigurace Port Trigger

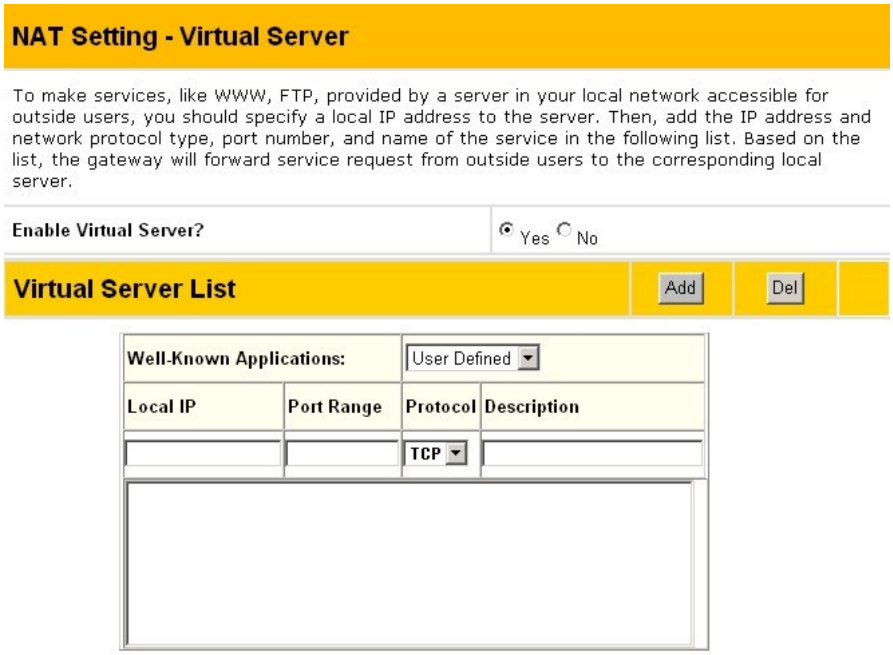
Některé aplikace vyžadují otevřený servisní port, jako jsou například internetové hry, video konference, internetová telefonie a mnoho dalších. Tyto aplikace nemohou pracovat s routerem, protože všechny porty jsou defaultně blokovány. Funkce Port Trigger umožňuje otevřít konkrétní TCP a UDP porty pro aplikace, které to vyžadují.

Enable Port Trigger?: Zapíná pravidla pro Trigger port.

Trigger Port List: Trigger Port je odchozí číslo portu, které je přiřazeno aplikaci.

Incoming Ports je specifické číslo portu, který je firewallem povolen na průchod skrz něj, když je detekován paket z triggeru.

NAT Setting-Virtual Server



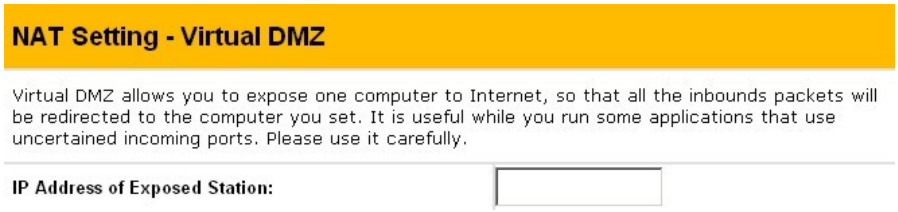
Obrázek 6.26: Konfigurace Virtual serveru

Virtual Server představuje možnost, jak na vaší intranetové síti provozovat služby dostupné z internetu. Virtual server nebo také přesměrování portu umožňuje přesměrovat všechen provoz z internetu na specifikovaný port (rozsah portů) na IP adresu ve vnitřní síti.

Enable Virtual Server?: Volba *Yes* zapíná funkci Virtuálního serveru

Virtual Server List: Local IP zde zadáte IP adresu počítače vnitřní sítě, kterému chcete umožnit přistup ze sítě internet. *Port range* zde zadáte číslo nebo rozsah portu, který budou přesměrovány na IP adresu počítače ve vnitřní síti.

NAT Setting- Virtual DMZ



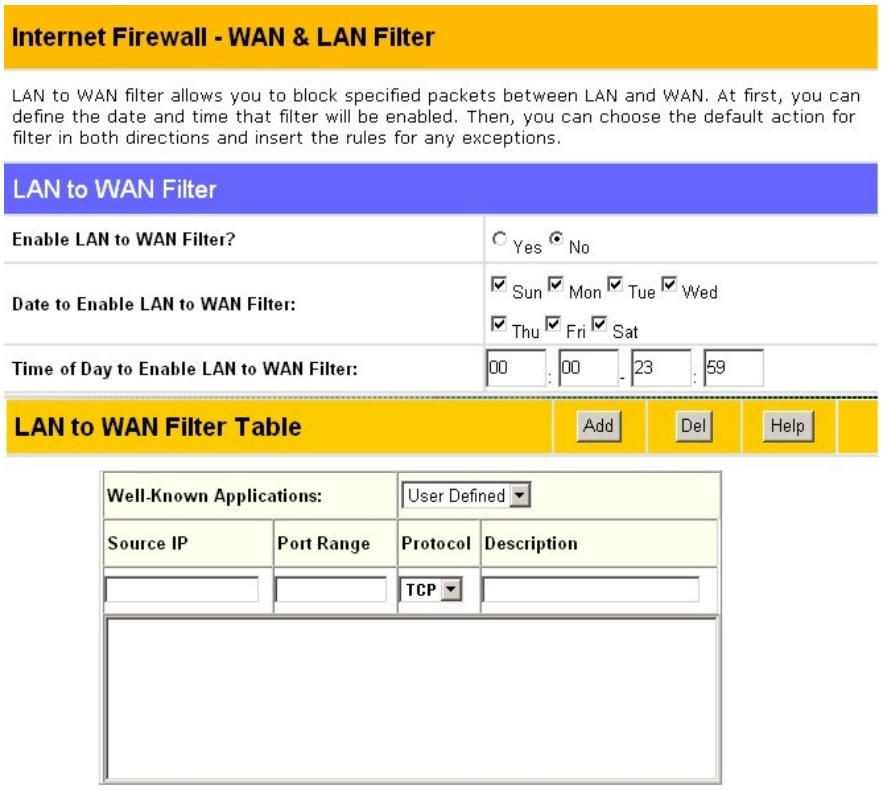
Obrázek 6.27: Nastavení demilitarizované zóny

Virtual DMZ představuje nastavení demilitarizované zóny, vyhrazuje IP adresu vnitřní sítě, na kterou se nevztahují restrikce definované přístupovým bodem. Provoz tohoto počítače je směřován bez jakéhokoliv omezení a není tak chráněn před případnými útoky z internetu. Většinou se do demilitarizované zóny umísťují počítače zajištující funkci webového serveru atp..

IP Address of Exposed Station: Do tohoto pole vyplňte IP adresu počítače, který chcete umístit do demilitarizované zóny.

6.1.2.3 Bezpečnost

Internet Firewall – WAN & LAN Filter



Obrázek 6.28: Filtrování služeb a přístupu na internet

Filtrování služeb a přístupu na internet umožňuje omezit přístup na internet v určitých dnech a hodinách, lze omezit přístup i na určité porty.

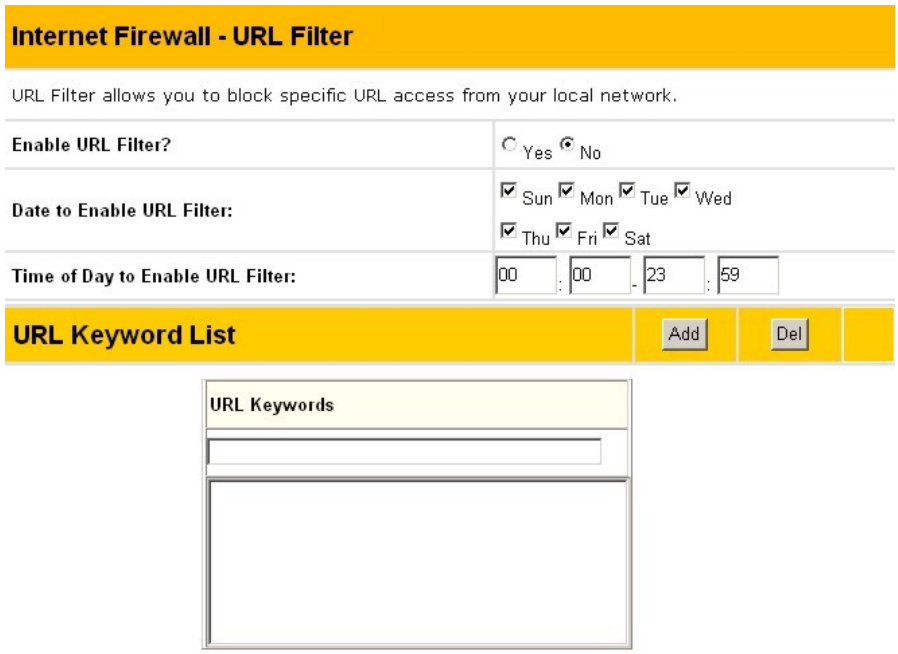
Enable LAN to WAN Filter?: Volba *Yes* zapíná službu LAN to WAN filtrů.

Date to Enable LAN to WAN Filter: Nastavení platnosti LAN to WAN filtrů na určité dny.

Time of Day to Enable LAN to WAN Filter: Nastavení platnosti LAN to WAN filtrů na určitý čas.

LAN to WAN Filter Table: Nastavení IP adres počítačů, rozsah portů pro které jsou filtry platné.

Internet Firewall – URL Filter



Obrázek 6.29: URL Filtr

URL Filtr nebo také filtr na základě obsahu kontroluje výskyt určitých slov na webové stránce nebo elektronické poště a zastaví inkriminovaný materiál dříve, než dorazí na chráněný počítač.

Enable ERL Filtr?: Volba *Yes* zapíná službu URL filtru.

Date to Enable URL Filtr: Nastavení platnosti URL filtru na určité dny.

Time of Day to Enable UTL Filtr: Nastavení platnosti URL filtru na určitý čas.

URL Keyword List: Nastavení klíčových slov na základě kterých budou data blokována.

6.1.2.4 Systémová nastavení

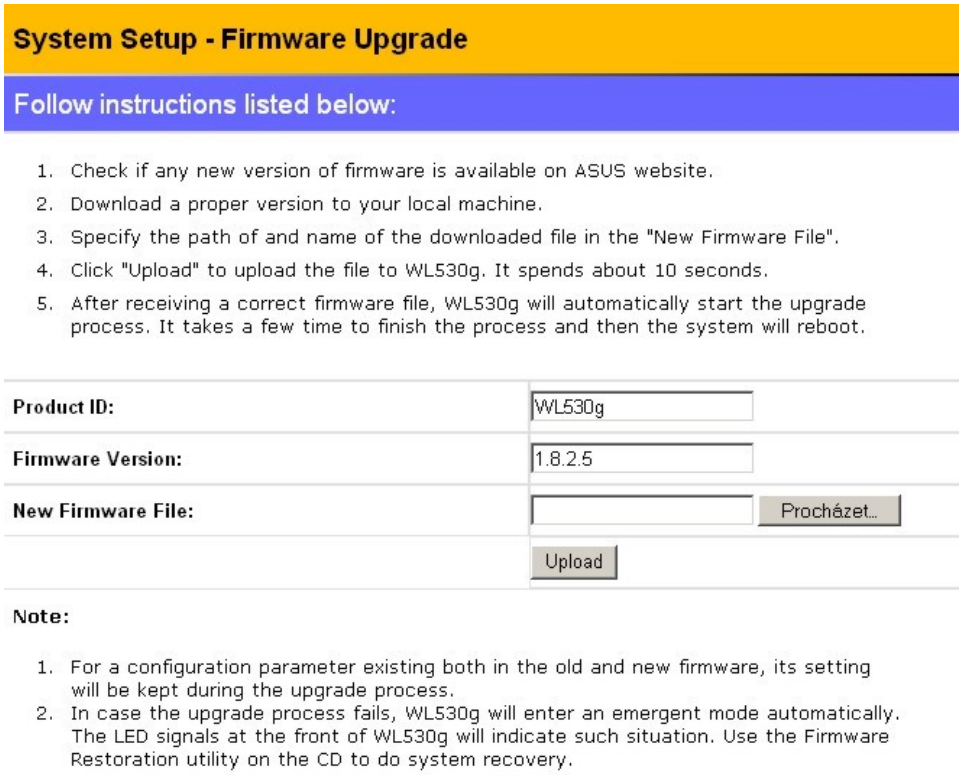
System Setup – Change Password

Obrázek 6.30: Nastavení uživatelského jména a hesla

New Password: Nastavte nové heslo přístupového bodu. Tovární heslo je "admin" a mělo by být co nejdříve nahrazeno novým heslem.

Retype New password: Potvrďte nové heslo.

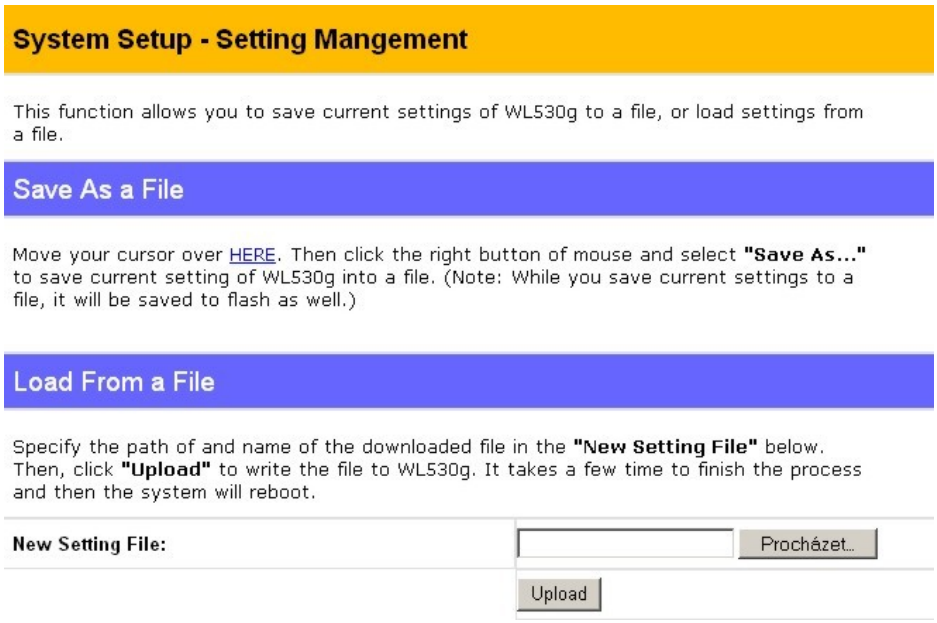
System Setup – Firmware upgrade



Obrázek 6.31: Aktualizace Firmwaru

Firmware Upgrade umožňuje upgrade (aktualizaci) vestavěného firmwaru vašeho přístupového bodu. Na webových stránkách výrobce daného přístupového bodu naleznete nové verze firmwaru i s popisem změn, které přináší oproti staré verzi. Firmware by měl být aktualizován co nejčastěji, optimální interval kontroly nových verzí firmwaru je 1-2 měsíce.

Systém Setup – Setting Manager



Obrázek 6.32: Systémová nastavení

Tato funkce vám umožní uložit aktuální nastavení přístupového bodu nebo načíst již uložené nastavení.

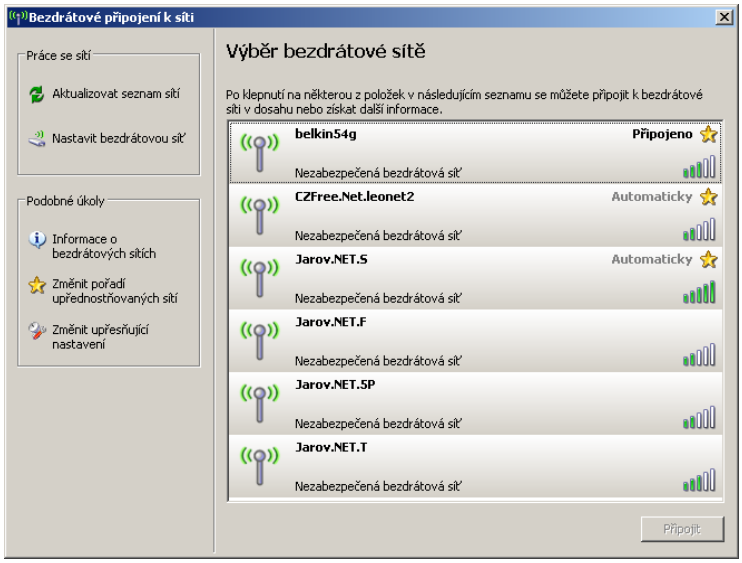
System Setup – Faktory Default

Obrázek 6.33: Systémová nastavení

Faktory Default vrátí všechny hodnoty nastavení na výchozí nastavení továrního nastavení.

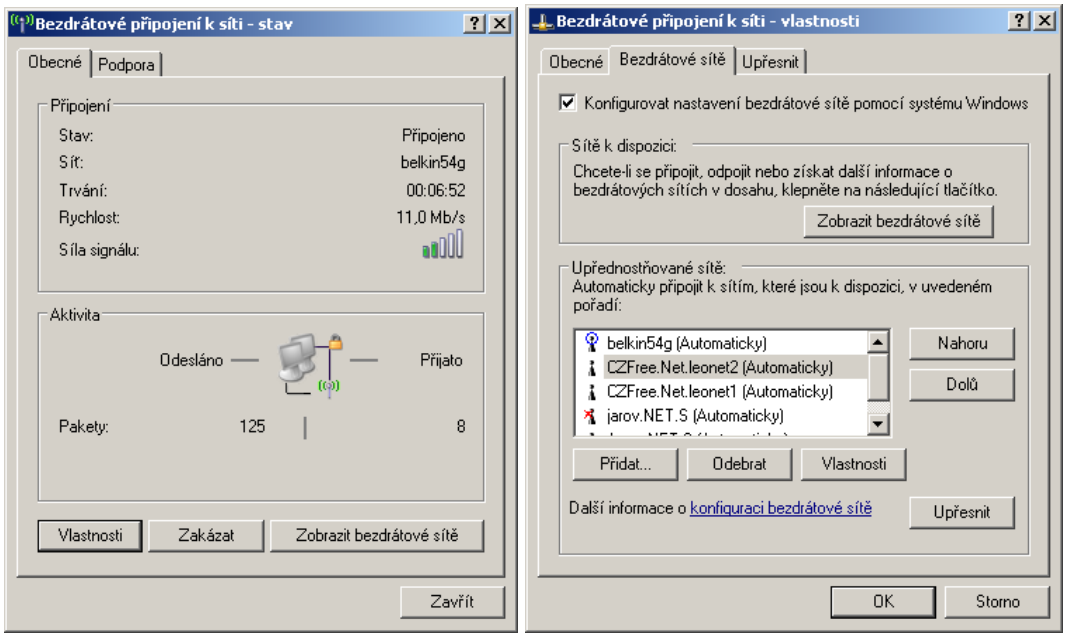
6.2 Konfigurace klienta

Bezdrátové síťové adaptery se z pohledu OS příliš neliší od klasických síťových adaptérů. Operační systém nevyžaduje žádné zvláštní prostředky k instalací bezdrátových klientů. Většinou si vystačí s protokolem TCP/IP, který je dostupný na každém moderním OS.
Nejrozšířenějším operačním systémem v současné době je OS Windows firmy Microsoft. Podpora bezdrátových sítí u tohoto operačního systému je přímo úměrná jeho stáří. OS Windows XP je v současné době nejnovějším operačním systémem řady Windows, jeho podpora bezdrátových zařízení je na dobré úrovni a podporuje i řadu dalších WiFi funkcí jako WPA zabezpečení či autentizaci 802.1x.
Výhodou Windows XP je funkce Zero Configuration, tedy absence manuální konfigurace. Po instalaci vaši WiFi karty OS sám prohledá dostupné WiFi sítě a nabídne připojení do nich.



Obrázek 6.34: Výběr bezdrátové sítě

Po připojení do bezdrátové sítě si můžete ještě otevřít okno se základním přehledem a možnostmi další konfigurace.



Obrázek 6.35: Základní přehled připojení k bezdrátové sítí, Vlastnosti konfigurace připojení k bezdrátové síti

Ve vlastnostech bezdrátových sítí si můžete nastavit například pořadí sítí, které má počítač volit pro připojování, takže pokud bude vaše oblíbená síť dostupná, připojíte se k ní automaticky.

6.3 Měření

Měření přijímaného výkonu probíhalo v bezdrátové datové síti nakonfigurované podle standardu 802.11b, kde je využívána vždy jedna konkrétní frekvence a je tak možné sledovat konkrétní pásmo. Pro analýzu přijímaného výkonu byly využity tři měřicí prostředky – karta D-link, a software NetStumbler spolupracující s interní bezdrátovou kartou notebooku.
Jako přístupový bod byl použit Access point společnosti *OvisLink* WMU-9000VPN s externí anténou MAXRAD profi sektor.anténa 13 dBi, H120° V16°. Jako klient bezdrátové sítě byl použit notebook UMAX 2400W,který sloužil k měření síly vysílání Access pointu.Software pro záznam a analýzu vysílaného výkonu byl nainstalován na notebooku UMAX 2400W. Karta D-link využívala externí anténu ANDREW 24dBi a program NetStumbler.Pro kvalitu signálu byly vzaty útlumy na konektorech a kabelu. Měření bylo prováděno na různých místech v oblasti požadovaného pokrytí.Anténa základnové stanice byla umístěna na střeše domu.

7 Závěr

V předložené bakalářské práci se zabývám obecnými principy tvorby bezdrátové sítě, především pak tvorbou sítě založené na standardu IEEE 802.11 neboli WiFi. Shrnuji zde poznatky týkající se návrhu, správy, zabezpečení a konkrétní realizaci této sítě. Při popisu služeb, které WiFi sítě používají se snažím především 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.
Rozvoj bezdrátových sítí zažívá v posledních několika letech velký rozmach. Výrobci WiFi zařízení vyvíjejí stále nové technologie standardy a normy. V těchto různých normách a standardech se uživatele poměrně těžko orientují. V úvodu této práce je proto věnována pozornost přehledu nejdůležitějších technologií, které jsou již dostupné i těch, které se připravují. Snahou bylo zachovat co největší aktuálnost, ovšem odvětví bezdrátové komunikace se vyvíjí v současné době velice rychle a je těžké odhadnout budoucí vývoj. I přes to práce obsahuje přehled nejdůležitějších technologií, které se v současné době pří realizaci WiFi sítí používají a je předpoklad, že se ještě nějakou dobu využívat budou.
Zvláštní pozornost jsem věnoval bezpečnosti WiFi sítí, což byla především zpočátku vývoje této technologie, často opomíjená kapitola. Masivní rozšíření WiFi sítí v posledních letech, mezi širokou veřejnost však ukázalo, že podcenění bezpečnosti WiFi síti má za následek odrazení většiny potencionálních firemních zákazníků. Na tuto situaci výrobci Wifi zařízení v posledních letech 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, pro něž je využití WiFi sítí zajímavou alternativou ke komerčním sítím, které využívají na rozdíl od WiFi licencovaná pásma.
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 také bylo hlavním cílem této bakalářské práce.

8 Seznam Literatury

1) HORST, J.: Informační a telekomunikační technika. Praha, BEN, 2004.ISBN 80-86706-08-7

2) KLAUS, T: Příručka pro elektrotechnika. Europa – Sobotáles, 2005.ISBN 80-86706-00-1

3) KOMAR, B.: Zabezpečení systému a sítě. Computer Press, 2007.ISBN 80-251-1260-8

4) PUŽMANOVÁ, R.:Moderní komunikační sítě od A do Z.Computer Press,2006.ISBN 80-251-1278-0

5) HORSKÝ, R.: Bezdrátové sítě Wi-Fi v rekordním čase. Grada, 2006.ISBN 80-247-1790-5

6) MICROSOFT PRESS: Základy sítí. Computer Press, 1999. ISBN 80-7226-158-4

7) BARKEN L.: Wi-Fi : jak zabezpečit bezdrátovou síť. Computer Press, Brno 2004.ISBN 80-251-0346-3

8) ZANDL P.: Bezdrátové sítě WiFi : praktický průvodce. Computer Press, Brno 2003. ISBN 80-7226-632-2

9) BRISBIN S.: Wi-fi : postavte si svou vlastní wi-fi síť. Neocortex, Praha 2002.ISBN 80-86330-13-3

10) Wikipedie otevřená encyklopedie <http://cs.wikipedia.org>

11) Access Server < http://access.feld.cvut.cz>

12) Živě <http://www.zive.cz>

9 Přílohy

9.1 Seznam obrázků

9.2 Slovník pojmů a zkratek

Acces Point - přístupový bod, řídí komunikaci mezi WiFi zařízeními
Ad-Hoc - WiFi síť bez přístupového bodu
Bluetooth - radiová bezdrátová norma
Bridge - síťový most, spojuje dva segmenty téže sítě
Channel - kanál frekvenčního pásma
ČTU - Český telekomunikační úřad
CSMA/CA - Carrier sense multiple access with collision avoidance, metoda vícenásobného přístupu s detekcí nosné a zabránění kolize
DHCP - Dynamic Host Configuration Protokol, protokol dynamické konfigurace stanice
DNS - Domain Name System, hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména
DSSS - Direct Sequence Spread Spektrum, rozprostřené spektrum přímé posloupnosti
ESS - Extend Service Set, překrývající se soubor služeb
FHSS - Frequency hopping spread spectrum, rozprostřené spektrum s přeskakováním mezi frekvencemi
Firewall - ochrana sítě před narušiteli, omezením přístupu na počítač nebo síť
IBSS - Independent Basic Service Set, viz. Ad-Hoc
IEEE 802.11 - Institute of Electrcal and Electronics Engineers, orgaizace která vytváří počítačové normy, 802 norma bezdrátových sítí, .11 norma WiFi sítí
IP - Internet Protocol, internetový protokol používaný všemi internetovými aplikacemi a používaný na lokákní a WiFi síti
ISP - Internet Service Provider, poskytovatel připojení k internetu
LAN - Local area network, lokální síť
MAN - Metropolitan Area Network, metropolitní sítě
NAT - Network Address Translation, překlad síťových adres
OFDM - Orthogonal Frequency Division Multiplexing, ortogonální frekcenční multiplex
OSI Model - Open systém Interconnect, propojení otevřených systémů
PAN - Personal Area Network, osobní síť
PCMCIA - Personal Computer Memory Card International Association, sběrnice kterou je vybavena většina notebooku
PCI - Peripheral Component Interconnect, sběrnice, kterou je vybavena většina osobních počítačů
PLCP - Physical Layer Convergence Protokol, protokol konvergence fyzické vrstvy
QoS - Quality of Service, služba zajišťující kavalitu hovorového a obrazového signálu
Roaming - pohyb bezdrátových zařízení mezi AP, která jsou nakonfigurována jako jediná síť
SSID - Service Set Identifer, identifikator souboru služeb
SSH - Secure Shell, klient/server protokol v síti TCP/IP

TCP - Transmission Control Protocol, vytváří virtuální okruh mezi koncovými aplikacemi, tedy spolehlivý přenos dat
USB - Universal Serial Bus, universální seriová sběrnice
VPN - Virtual private network, virtuální privátní síť
WAN - Wide Area Network, rozsáhlé sítě
WLAN - Wireles Local Area Network, bezdrátové lokální sítě
WECA - Wireless Ethernet Compatibility Alliance, Aliance pro kompatibilnost bezdrátového ethernetu
WEP - Wired Equivalent Privacy, bezpečnostní mechanizmus
WiFi - Wireles Fidelity, označení pro výrobky vyhovující podmínkám WiFi Aliance