UNIVERZITA PARDUBICE
ÚSTAV ELEKTROTECHNIKY A INFORMATIKY

Návrh počítačové sítě s využitím WiFi technologie

BAKALÁŘSKÁ PRÁCE

2007 **Křížek Tomáš**

UNIVERZITA PARDUBICE
ÚSTAV ELEKTROTECHNIKY A INFORMATIKY

Návrh počítačové sítě s využitím WiFi technologie

BAKALÁŘSKÁ PRÁCE

AUTOR PRÁCE: Křížek Tomáš
VEDOUCÍ PRÁCE: Ing. Miloslav Macháček

2007

UNIVERSITY OF PARDUBICE
INSTITUTE OF ELECTRICAL ENGINEERING AND INFORMATICS

The Project of Computer Network with Application of WiFi Technologies

BACHELOR WORK

AUTHOR: Křížek Tomáš
SUPERVISOR: Ing. Miloslav Macháček

2007

Vysokoškolský ústav: Ústav elektrotechniky a informatiky
Katedra/Ústav: Ústav elektrotechniky a informatiky
Akademický rok: 2006/2007

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Pro: Křížek Tomáš

Studijní program: Informační technologie

Studijní obor: Informační technologie

Název tématu: Návrh počítačové sítě s využitím WiFi technologie

Zásady pro zpracování:

Teoretická část bude obsahovat zdůraznění významu propojení osobních počítačů do sítě, popis typů sítí, síťových komponent (AP, klient, router, switch, repete, bridge a další) se zaměřením na komponenty WiFi sítě. Implementační část bude postavena na prezentaci návrhu topologie počítačové sítě s využitím WiFi technologie a popisem nastavení jednotlivých komponent.

Seznam odborné literatury:

Základní:

- Wendell Odom, *Počítačové sítě bez předchozích znalostí,* Computer Press: 2005
- Patrick Zandl, *Bezdrátové sítě WiFi – Praktický průvodce,* Computer Press: 2003

Rozsah: přibližně 40 stran

Vedoucí práce: Ing. Miloslav Macháček

Vedoucí katedry (ústavu): prof. Ing. Pavel Bezoušek, CSc.

Datum zadání práce: 30. 11. 2006

Termín odevzdání práce: 12. 5. 2007

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona a.121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně Univerzity Pardubice.

V Pardubicích dne 10. 5. 2007

Křížek Tomáš

Poděkování:

Rád bych poděkoval Ing. Miloslavu Macháčkovi za odborné rady a vedení při zpracování bakalářské práce.

ABSTRAKT

Tato práce si klade za cíl vytvořit návrh počítačové sítě s použitím technologie WiFi.

V prvé části práce je popsána historie vzniku bezdrátových sítí, princip jejich funkce, nejpoužívanější standardy, zabezpečení bezdrátových sítí, popis základních aktivních síťových prvku. Některá z těchto zařízení jsou použita v samotném návrhu sítě.

Ve druhé části je popsán konkrétní návrh počítačové sítě v podniku. Součásti návrhu je konkrétní popis nastavení na použitých zařízeních.

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek a pojmů

WiFi	Wirelless Fidelity - zkratka pro bezdrátové sítě
LAN	Local Area Network – lokální počítačová síť
Broadcast	Všesměrová adresa
Bit	Binární číslo - jednička nebo nula
Byte	Jednotka osmi binárních číslic, označovaná též jako znak nebo oktet
MIMO	Multiple input multiple output - použití vícecestné propagace pomocí více přijímacích a vysílacích antén
Ethernet	Technologie přenosu dat po kabelovém vedení nečastěji kroucené dvoulince, ale i jiných typech kabelů
SSID	Service Set Identifier – identifikátor bezdrátové sítě
TCP/IP	Sada protokolů pro komunikaci v počítačové síti
MAC adresa	Jedinečný identifikátor síťového zařízení
Firmware	Speciální software uložený v ROM paměti zařízení, které je integrální součástí elektronického zařízení
NAT	Network Adress Translation (překlad síťových adres)
Embedded systém	Jednoúčelový systém, ve kterém je řídicí počítač zcela zabudován do zařízení, které ovládá
Server	Zařízení poskytující v síti specifické služby
VLAN	Virtuální LAN - skupina zařízení v jedné nebo více lokální síti, která jsou zkonfigurována tak, že mohou komunikovat jakoby byly připojeny k jednomu síťovému segmentu

1 Úvod

V dnešní době představuje pojem počítačová síť jednoznačně fenomén. První pokusy se vzájemnou komunikací počítačů se datují do 60.let 20.století. Tehdy šlo pouze o pokusy, přičemž se zjišťovalo k čemu by toto spojení mohlo být v budoucnu dobré.

Postupně byly objevovány nové možnosti využití plynoucí ze spojení a vzájemné komunikace více počítačů. Ani dnes ještě stále není výčet možností konečný a jsou stále hledány nové možnosti využití.

S tím jak rostlo povědomí, podpora a kvalita, tím více se počítačové sítě dostávaly do povědomí lidi, pro které byla možnost ulehčit si a zefektivnit práci vítána. Proto asi nepřekvapí, že dnes můžeme počítačové sítě najít prakticky v kterémkoliv podniku či domácnosti. Postupné vzájemné propojování sítí dalo vzniknout celosvětové počítačové sítí, která dostala název Internet.

Osobně mám zkušenosti s budováním počítačových sítí, neboť v místě mého bydliště se podílím na projektu broadband telekomunikační sítě. Z těchto důvodů jsem si i vybral tuto práci, neboť se o problematiku počítačových sítí zajímám, a dá se říci, že je i jednou z mých zálib. V budoucnu bych se chtěl této oblasti věnovat i profesně.

Úkolem je tedy vytvořit návrh počítačové sítě s použitím WiFi technologie. V úvodu této práce nejprve uvedu základní informace o důvodu vzniku bezdrátových sítí, principu jejich funkce, uvedu standardy, které jsou dnes nejpoužívanější, krátce se zmíním a vysvětlím funkci základních síťových prvků, bez kterých by budování sítí nebylo možné.

Samotný návrh budoucí sítě bude představovat konkrétní realizaci počítačové sítě pro firmu HPh. Tento podnik se má stěhovat do nových prostor, a proto je potřeba vytvořit novou vnitropodnikovou síť.

2 Základní informace

2.1 Význam propojení více PC

Počítačová síť je spojení dvou a více počítačů. Toto spojení se provádí za účelem vzájemného sdílení jak hardwarových tak softwarový prostředků.

Jako příklad lze uvést například společné sdílení tiskáren, faxu, scanneru, úložného prostoru pro data jednotlivých uživatelů a možnost komunikace mezi uživateli.

2.2 Vznik bezdrátových síti

První bezdrátové sítě původně vznikly jako doplňková řešení LAN sítí pro potřebu omezené mobility uvnitř objektů, většinou kanceláří. Tyto sítě mohly klasickým drátovým LAN sítím konkurovat velice těžko. Určitě ne cenou a alespoň ze začátku ani rychlostmi. Klasickým sítím ovšem konkurovaly svým samotným principem funkce - bezdrátovým charakterem.

Uplatnění takových sítí bylo především tehdy, když se uživatel potřeboval často přemísťovat nebo klasické kabeláže (například v přísně chráněných památkových objektech) nebo v situaci, kdy bylo třeba zřídit lokální síť jen na velmi dočasnou dobu, a pak vše rychle uvést do původního stavu. Ve výsledku tak byly bezdrátové lokální sítě spíše výjimkou.

Postupem času však došlo k zdokonalování technologií – rychlosti se zvyšovaly, dosah se zvětšoval a ceny zařízení klesaly.

Dalším impulsem pro rozvoj bezdrátových sítí byl stále větší prodej mobilních zařízení (notebooku, PDA). Uživatelé těchto zařízení požadovali mobilitu, kterou přinášela právě bezdrátová technologie.

Hlavní přednosti bezdrátových lokálních sítí

- Mobilita uživatelů - bez jakýchkoliv "drátů" s možností přesně vykrýt pouze ty prostory, které mají být vykryty
- Rychlost bezdrátových datových přenosů postačuje pro běžné kancelářské použití (nejpoužívanější standardy 802.11b a 802.11g).
- Snadnost a rychlost vybudování bezdrátové sítě - žádné sekání zdí, žádná pokládka kabelů, možno rychle zřídit i rychle uvést do původního stavu.

2.3 WLAN

WLAN je zkratka anglických slov Wireless Local Area Network nebo též Wireless LAN. Znamená „bezdrátová místní síť“.

Je to typ místních sítě, které jako přenosové médium používají elektromagnetické rádiové vlny v pásmech řádu GHz. Je pro ně typické sdílení média a princip CSMA/CA, na rozdíl od CSMA/CD např. u Ethernetu.

2.4 WLAN podle IEEE

IEEE (Institute of Electrical and Electronics Engineers) se zabývá specifikací bezdrátových LAN. Začátky této činnosti se datují přibližně okolo roku 1990. Jedná se o následující podvýbory:

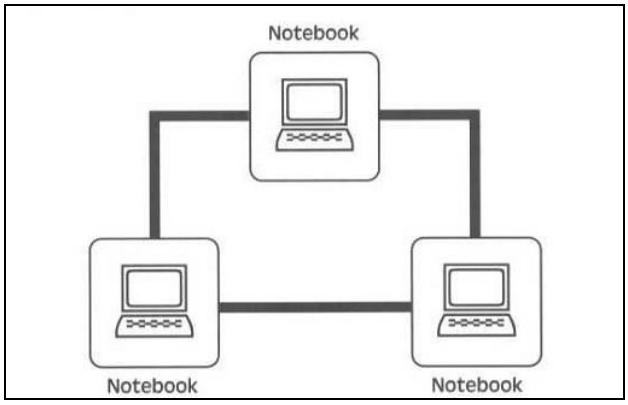
- IEEE 802.11 - Bezdrátové lokální sítě (Wireless Local Area Network, WLAN)
- IEEE 802.15 - Bezdrátové osobní sítě (Wireless Personal Area Network, WPAN)
- IEEE 802.16 - Širokopásmový bezdrátový přístup (bezdrátové metropolitní sítě)

2.5 Standard IEEE 802.11

2.5.1 Typy sítí

Technologie IEEE 802.11 je určena hlavně pro výstavbu lokálních radiových sítí s infrastrukturou.

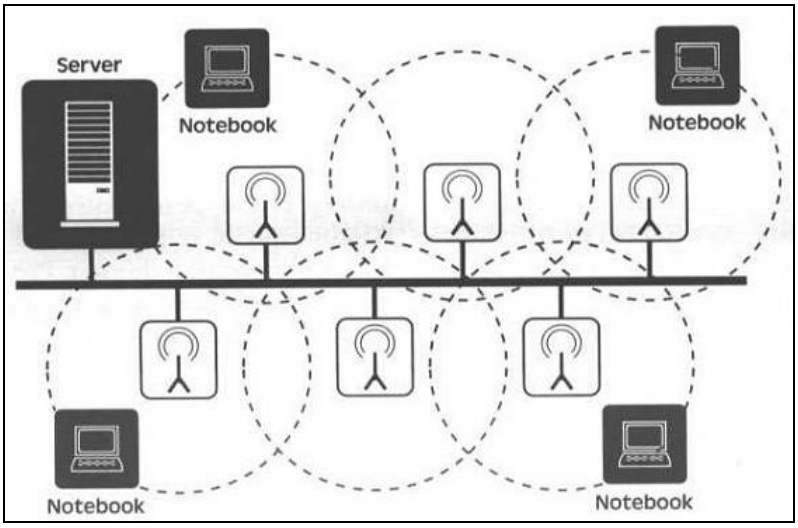
Ad-hoc sítě – jednotlivé stanice v takové síti spolu komunikují přímo mezi sebou. Z toho plyne, že vzájemná komunikace je možná pouze pokud jsou ve vzájemném radiovém dosahu. Toto řešení je vhodné pro síť, kde se předpokládá pouze několik stanic s podmínkou malé vzdálenosti mezi nimi, proto je možné použít tento typ sítě v menších prostorech například v kancelářích. Ad-hoc komunikace má větší nároky na klienta, který udržuje spojení s každou komunikující stanicí.



Obr.1 Princip komunikace stanic v síti typu Ad-hoc (1)

Infrastrukturní sítě – mají svoji přesně danou infrastrukturu, existuje zde centrální prvek tzv. přístupový bod (access point). Přístupový bod je tedy vlastně rozhraní mezi drátovou a bezdrátovou sítí.

Přístupový bod jako takový je schopen komunikovat a obsloužit více stanic – klientů najednou. Samotná komunikace neprobíhá přímo mezi stanicemi, ale prostřednictvím přístupového bodu. Proto v této síti může fungovat každá stanice, která dokáže komunikovat s přístupovým bodem a nachází se v místě, kde lze zachytit signál přístupového bodu.



Obr.2 Princip komunikace stanic v síti typu infrastruktura (2)

2.5.2 Původní standard IEEE 802.11

Základem pro výstavbu lokálních bezdrátových sítí se stal standard IEEE 802.11 vytvořený v polovině devadesátých let. Vznikla tak bezdrátová alternativa (drátového Ethernetu), která pracuje v bezlicenčním pásmu 2,4 GHz.

Standard 802.11 také definuje fungování "bezdrátového Ethernet" na podvrstvě MAC (Media Access Layer), řídící přístup ke sdílenému přenosovému médiu.

Oproti klasickému „drátovému“ Ethernetu nelze použít přístupovou metodu CDMA/CD z důvodu nemožnosti detekce kolizí. Uzel, který vysílá, není schopen spolehlivě detekovat současné vysílání ostatních uzlů, a proto byla použita úplně jiná přístupová metoda, která vzniku kolizí předchází, a vůbec neumožňuje jejich výskyt.

Metoda se nazývá CDMA/CA (Carrier Sense, Multiple Access with Collision Avoidance). Princip funkce je takový, že uzel, který chce odeslat data, nejprve vyšle krátký paket RTS (Request to Send) s údajem o velikosti hlavního datového paketu. Pokud příjemce žádost RTS zaslechne, odpoví na ni paketem CTS (Clear to Send). Poté zdrojový uzel skutečně odešle svá hlavní data, na-

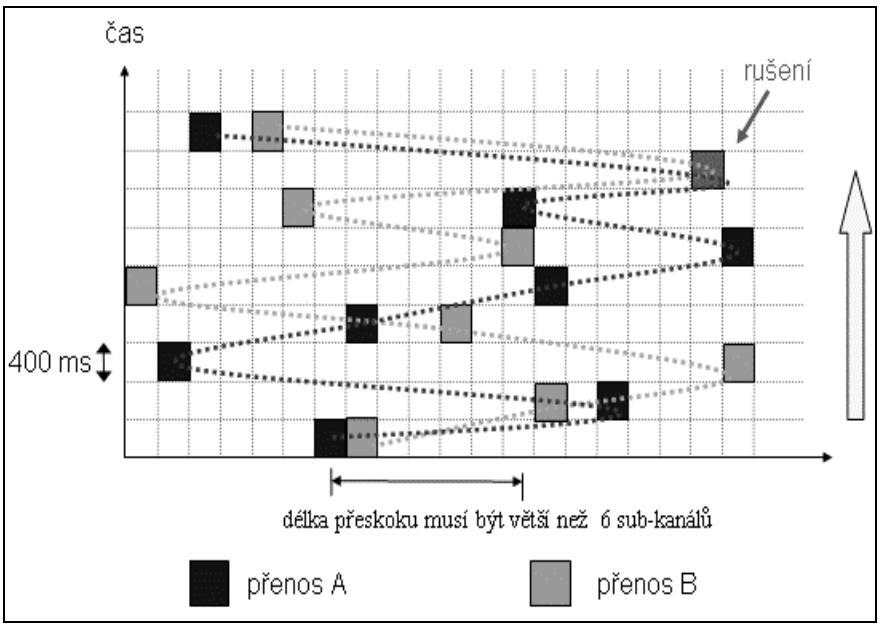
čež si počká na potvrzení příjemce (ACK). Ten kontroluje správnost přijatých dat hlavně podle kontrolního součtu (přesněji CRC).

Bezdrátová zařízení využívají pro přenos dat frekvenci v řádu GHz. U signálu s takovou frekvencí se setkáme s některými nepříjemnými problémy.

2.5.3 Typy rozprostřeného spektra

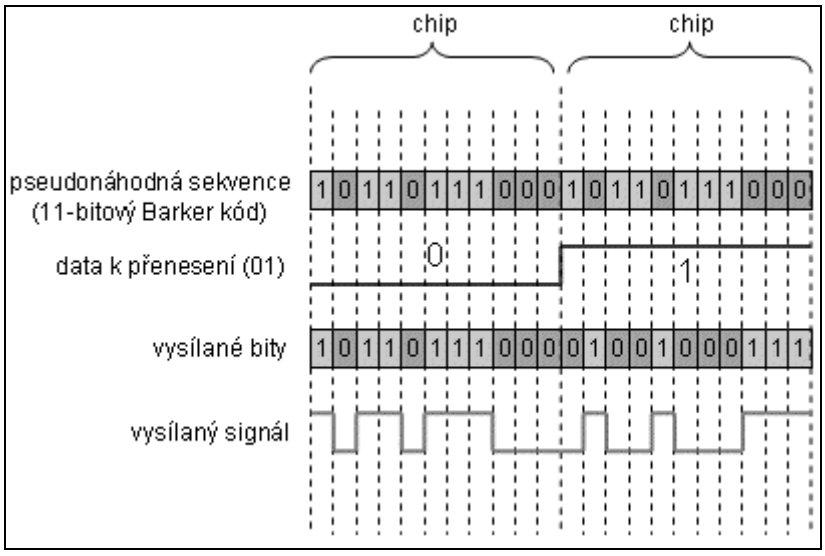
Radiová fyzická vrstva standardu 802.11 definuje tři různé techniky rozprostřeného spektra.

Frekvenční proskoky (Frequency hopping FHSS) - vysílač skáče v pseudonáhodném pořadí po frekvenčních pásmech a na každém vysílá krátký datový proud. Frekvenční šířka celého pásma je 83,5 MHz. Toto pásmo je rozděleno na 79 kanálů o šířce 1MHz. Signál přeskakuje v náhodném pořadí po těchto kanálech. Výhodou je větší počet systému pracujících v jednom pásmu. Teoreticky je možný provoz 26, prakticky ale jen okolo 15 přístupových bodů.



Obr.3 Přenos signálu pomocí frekvenčních proskoků (3)

Přímá sekvence (Direct Sequence – DS, DSSS) - pracuje na principu, že každý jednotlivý bit určený k přenosu, je nejprve nahrazen určitou početnější sekvencí bitů (tzv. chipů). Tyto sekvence mají nejčastěji pseudonáhodný charakter. Přenášena je pak tato sekvence bitů. Jde tedy vlastně o umělé zavedení nadbytečnosti (redundance), podobné tomu, které se při datových přenosech někdy používá pro zajištění větší spolehlivosti přenosů. Důvod pro zavedení redundance je zde jiný. Signál je rozprostřen do větší části radiového spektra, je méně citlivý vůči rušení (což zvyšuje spolehlivost přenosu). Signál se ostatním uživatelům jeví jako náhodný šum a bez znalosti mechanismu vytváření původní pseudonáhodné sekvence, je pro ně obtížné zpět získat (demodulovat) přenášená data.



Obr.4 Způsob přenosu signálu u DSSS (4)

Ortogonální frekvenční multiplex (OFDM - Orthogonal Frequency Division Multiplexing) - Jde o přenosovou techniku pracující s tzv. rozprostřeným spektrem, kdy je signál vysílán na více nezávislých frekvencích, což zvyšuje odolnost vůči interferenci.

Datový tok daného kanálu je rozdělen na stovky dílčích datových toků jednotlivých nosných kmitočtů.

Díky tomu je na přijímací straně možné potom právě vysílaný symbol nerušeně přijmout, i když přichází k přijímači více cestami s různým zpožděním.

OFDM byla přijata jako standard IEEE 802.11a pro pásmo ISM 5 GHz, v roce 2003 byla také implementována pro pásmo ISM 2,4 GHz jako 802.11g.

2.5.4 Dostupné radiové frekvence

Pro standard 802.11b a 802.11g je vyhrazeno pásmo 2,4 GHz, u standardu 802.11a je pásmo souhrnně označováno jako 5 GHz.

V zemích Evropské unie se provozuje 802.11a na frekvencích 5,47 – 5,725 GHz .

U standardů 802.11b, 802.11g jde o následující frekvence.

Tabulka č.1. Rozdělení kanálů podle standardu (1)

Kanál	Frekvence (GHz)	Kanál	Frekvence (GHz)
1	2,412	*8*	2,447
2	2,417	*9*	2,452
3	2,422	*10*	2,457
4	2,427	*11*	2,462
5	2,432	*12*	2,467
6	2,437	*13*	2,472
7	2,442	*14*	2,484

Použití kanálů v jednotlivých zemích. Technologie rozprostřeného spektra využívá pásmo o velikosti 22 MHz a odstup mezi kanály je 5 MHz.

Z toho vyplývá, aby se dva přístupové body navzájem nerušily a nepřekrývaly, musí být nastaveny minimálně o pět kanálů od sebe.

Tabulka č.2. Rozdělení kanálů podle standardu (2)

Země	Kanály
USA a Kanada	1-11 (2,412 – 2,462 GHz)
Evropa mimo Španělsko a Francii	1-13 (2,412 – 2,472 GHz)
Francie	10-13 (2,457 – 2,472 GHz)
Španělsko	10-11(2,457 – 2,462 GHz)
Japonsko	14 (2,482 GHz)

2.6 IEEE 802.11b

Původní norma pro WLAN (802.11) byla doplněna o rozšíření, které vyřešilo největší problém, což byla nízká přenosová rychlost. "Rychlé rozšíření" (High Rate, HR) základní normy IEEE 802.11b (1999), přezdívané také Wi-Fi (Wireless Fidelity), přichází s vyššími rychlosti v pásmu 2,4 GHz, a to až 11 Mbit/s.

Pro jejich dosažení využívá nový způsob kódování, tzv. doplňkové kódové klíčování (Complementary Code Keying, CCK) v rámci DSSS na fyzické vrstvě.

Podle momentální rušivosti prostředí se dynamicky mění rychlost na nižší nebo naopak na vyšší: 11 Mbit/s, 5,5 Mbit/s, 2 Mbit/s až 1 Mbit/s. Maximální rychlost na fyzické vrstvě je sice 11 Mbit/s, ale užitná rychlost je nižší, protože 30-40 procent teoretické kapacity tvoří režie.

Uživatelská rychlost se udává většinou okolo 6 Mbit/s. 802.11b není dobře přizpůsobena k přenosu hlasu, což je dáno především velmi variabilním zpožděním při přenosu paketu - a to je vlastnost, která souvisí s CSMA/CA jako metodou řízení přístupu.

2.7 IEEE 802.11g

IEEE 802.11g je navržen pro bezlicenční pásmo 2,4 GHz stejně jako WiFi (802.11b). Maximální rychlostí na fyzické vrstvě byla zvýšena na teoretických 54 Mbit/s (stejně jako tomu je u standardu 802.11a). Stejně jako 802.11b může 802.11g podporovat maximálně tři nepřekrývající se kanály. Podobný je i dosah sítě (při nastavení stejných rychlostí jako u 802.11b, s vyššími rychlostmi klesá dosah u 802.11g pouze na 30 metrů). Jedním z hlavních cílů u 802.11g byla (kromě zvýšení rychlosti) zpětná slučitelná s 802.11b. Díky tomu v jedné síti mohou fungovat klienti obou typů sítí. Oba standardy se liší řešením fyzické vrstvy: 802.11b používá DSSS a 802.11g OFDM (pro zpětnou kompatibilitu s 802.11b navíc také DSSS).

Dnes s největší pravděpodobností nejrozšířenější standard pro vnitřní přístupové body.

2.8 IEEE 802.11a

WLAN IEEE 802.11a pracuje v pásmu 5 GHz s vyšší teoretickou rychlostí, než je tomu u standardu 802.11b. Teoretická rychlost je 54 Mbit/s. Diky režii spojené s přenosem je reálná rychlost přenosu okolo 25 Mbit/s. Pro přenos se používá ortogonální multiplex s kmitočtovým dělením (Orthogonal Frequency-Division Multiplexing, OFDM).

Výhoda 802.11a oproti 802.11b spočívá nejen ve vyšších rychlostech, ale také v použité frekvenci: frekvence 5 GHz je méně vytížena a dovoluje využití více kanálů bez vzájemného rušení. Rozdílně využívané kmitočty u obou typů WLAN znemožňují jejich vzájemnou spolupráci. Podle definice standardu 802.11a je k dispozici osm nezávislých, nepřekrývajících se kanálů.

2.9 IEEE 802.11n

Tento standard upravuje fyzickou vrstvu a podčást linkové vrstvy, takzvanou MAC(Media Access Control) podvrstvu tak, aby bylo docíleno reálné rychlosti přes 100 Mbit/s. Do budoucna se počítá s maximální rychlost až 540 Mbit/s. Současně se zvýšením rychlosti se má zvýšit dosah.

Standard je stále ve vývoji. Základem je technologie MIMO (multiple-input multiple-output). Přenos dat je rozdělen na více toků a následně se odesílají data přes dvě či více antén. Jednotlivé datové toky jsou pak přijaty jinými anténami a převedeny zpět na tok prvotní. Bezdrátová komunikace s MIMO využívá vícecestné propagace (multipath) k zvýšení propustnosti a dosahu, nebo k snížení počtu přenosových bitových chyb.

Ke schválení standardu 802.11n verze1 došlo v březnu 2006. Podle dostupných informací se ratifikace standardu 802.11n očekává na jaře 2008. Již dnes se můžeme setkat s prvními implementacemi u bezdrátových zařízení na trhu.

2.10 Přehled parametrů vybraných standardů

Zde je uveden přehled technických parametrů pro jednotlivé standardy.

Tabulka č.3 Porovnání WLAN(3)

Typ	Kmitočet	Teoretická rychlost	Reálná rychlost	Přenos
802.11b	2,4 – 2,485 GHz	11 Mbit/s	~ 6Mbit/s	DSSS
802.11g	2,4 – 2,485 GHz	54 Mbit/s	~ 22Mbit/s	OFDM/ DSSS
802.11a	5,1 – 5,3 GHz 5,725 – 5,825 GHz	54 Mbit/s	~ 25Mbit/s	OFDM

3 Zabezpečení sítí 802.11

3.1 Důvod zabezpečení

Z principu funkce bezdrátové sítě nelze dostatečně přesně omezit prostor, kde bude signál k zachycení. V případě odposlouchávání v kabelové sítí je nejprve nutné se dostat fyzicky k samotným kabelům, naproti tomu v případě bezdrátových sítí se stačí dostat k odposlechu do prostoru, kde lze zachytit signál.

U provozu v drátových sítích přepínače posílají data pouze na cílový počítač. V radiové síti je zachytitelný veškerý provoz od všech počítačů, které spolu bezdrátově komunikují.

Pomocí programu, které lze stáhnout z Internetu, lze získávat pak tato přenášená data a dostávat se k těmto citlivým informacím.

Bezpečnost v bezdrátových sítí se rozděluje do dvou skupin:

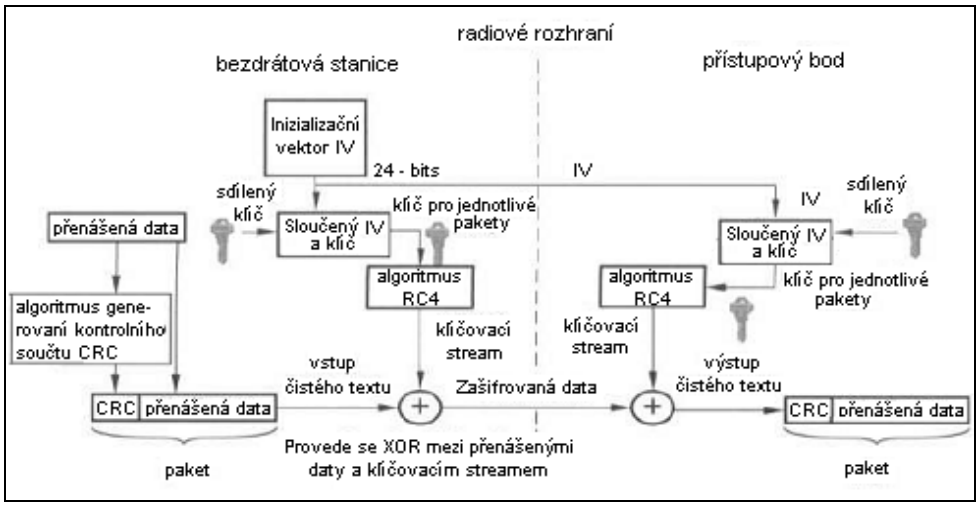
- šifrování – zabezpečení přenášených dat před odposlechem
- autorizace – řízení přístupu oprávněných uživatelů

3.2 Zabezpečení přenášených dat

Bezdrátová síť standardu 802.11 již od doby svého vzniku nabízela volitelné šifrování právě z důvodu důvěryhodnosti.

WEP(Wired Equivalent Privacy) - je součástí IEEE 802.11 standardu od roku 1999. Původním předpokladem bylo poskytnout stejné zabezpečení, jaké běžně poskytují drátové sítě. Informace v bezdrátových sítích jsou ale přenášena vzduchem a proto je snadné je odposlouchávat.

Pro šifrování metodou WEP se využívá proudová šifrovací metoda RC4 pro utajení informací. Pro ověření jejich správnosti používá metodu CRC-32 kontrolního součtu.



Obr.5 WEP zabezpečení pomocí algoritmu RC4 (5)

64 bitový WEP – z 64 bitů používá - 40 bitů pro klíč, zbylých 24 bitový je inicializační vektor, který poté dohromady tak právě tvoří 64 bitový RC4 klíč.

128 bitový WEP – ze 128 bitů používá – 104 bitů pro klíč, zbylých 24 bitový je inicializační vektor, který pak dá dohromady tak tvoří 128 bitový RC4 klíč.

256 bitový WEP - implementuji pouze někteří výrobci bezdrátových zařízení. 232 bitů je určeno pro klíč, zbylých 24 bitů je inicializační vektor.

WEP zabezpečením lze proniknout právě díky chybě v implementaci – rozkódování není těžké, ale právě díky bitové délce časově náročné. V době vzniku specifikace nebyla výpočetní technika tak výkonná, takže se tento problém nijak intenzivně neřešil. Dnes však již představuje riziko, protože dnes je možné použít metodu hrubé síly a v reálném čase dekódovat zabezpečená data. Proto je vhodné WEB kombinovat s některou další metodou zabezpečení (například kontrola MAC adres síťových karet klientů). Přes všechny tyto možnosti se použití zabezpečení pomocí WEP nedoporučuje.

WPA (Wi-Fi Protected Access) – toto zabezpečení vzniklo právě kvůli zvyšujícímu se riziku při používání zabezpečení WEP, kde hrozila možnost zneužití bezpečnostních nedostatků. Snahou bylo vytvořit standard, který by mohl využít hardware podporující WEP, ale vhodnými doplňkovými mechanismy (především prací s klíči) eliminovat jeho slabá místa. Standard WPA vznikl jako dočasné řešení do doby, než bude dokončena specifikace 802.11i.

Ze specifikace 802.11i byly pro WPA použity mechanizmy šifrování a řízení přístupu do bezdrátové sítě. Pro šifrování je použit TKIP.

- TKIP (Temporal Key Integral Protocol) – používá stejné šifrování jako WEP tedy 128 bitový klíč, ale na rozdíl WEP dochází k dynamické změně dočasného klíče. TKIP má implementován automatický mechanismus, který každých 10 000 paketů změní dočasný klíč. Dalším bezpečnostním mechanismem TKIP je MIC (Message Integrity Check), který kontroluje integritu zpráv. MIC má za úkol znemožnit útočníkovi během přenosu změnit zprávu. Přes všechna vylepšení se jedná pouze o překlenovací řešení. Problém by měl vyřešit standard 802.11i

WPA2/IEEE 802.11i(Wi-Fi Protected Access 2) - jedná se o komplexní řešení zabezpečení pro všechny sítě standardu 802.11. Byl navržen nový protokol CCMP pro silné šifrování pomocí AES (Advanced Encryption Standard). Volitelně je možné pro zpětnou slučitelnost použit starší WPA, která používá protokol TKIP s šifrováním pomocí RC4. Tuto šifru používal i nejstarší WEP.

Protokol CCMP (Counter-mode CBC – Cipher Block Chaining) MAC (Message Authentication Code) Protocol) dynamicky regeneruje 128 bitové klíče a přitom kontroluje integrity zpráv (MIC, kontrolní pole má délku 64 bitů) a čísluje pakety na ochranu proti útokům typu Replay.

Norma nabízí řadu dalších volitelných prvků, jako pre-authentication a key-caching, které nabízí rychlý a bezpečný roaming mezi přístupovými body (důležité pro hlasové služby po WLAN).

Standard 802.11i má za cíl minimalizovat útoky na bezpečnost WLAN. Dokáže ochránit před útoky man-in-the-middle. Navíc stále není vyřešena hrozící krádež identity v souvislosti s krádežemi zařízení, kde jsou uloženy identifikační údaje v cache.

AES je zatím neprolomitelný šifrovací algoritmus, takže utajení dat je spolehlivé. WPA2 je zpětně kompatibilní s WPA, takže souběžné použití WPA a WPA2 je v sítích běžné (na rozdíl od nepřijatelné kombinace WPA2/WEP).

3.3 Autentizace

Důležitou součástí bezpečnostní strategie je autentizace uživatele. U bezdrátové sítě nelze přesně vymezit prostor, kde všude bude signál přístupového bodu dostupný, a proto nelze nikdy prostor zcela kontrolovat proti průniku nepověřených osob. Naopak přístup oprávněných osob do vykrývaného prostoru je jednou ze základních důvodů (mobilita), proč bezdrátové sítě vznikly.

Standard 802.11 definují dvě metody autentizace:

- Open-systém autentizace
- Shared-key autentizace

Autentizace v bezdrátové síti je jednosměrný proces. Pracovní stanice (klient) musí požádat o autentizaci, přičemž z toho automaticky nevyplývá, že tuto autentizaci dostane.

Open-systém autentizace - jediná metoda vyžadovaná původním standardem 802.11. Způsob autentizace spočívá v tom, že přístupový bod přijme údaje poskytnuté klientskou stanici, aniž by je jakkoliv ověřoval. Zároveň přístupový bod vysílá svoje SSID

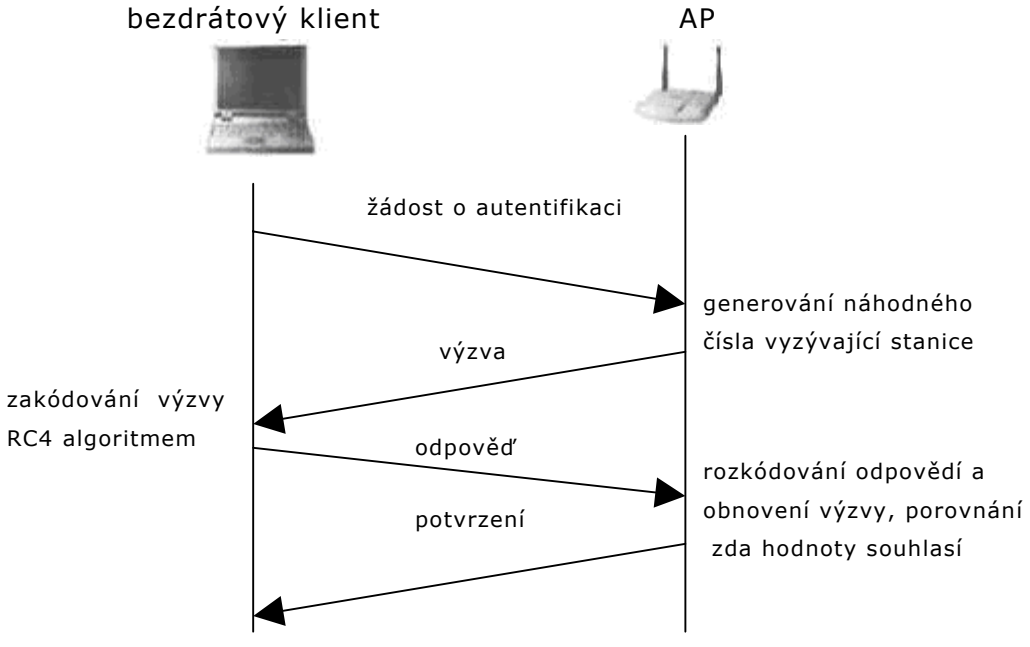
(Service Set Identifier), pokud není úmyslně skryto z důvodu omezení přístupu. Stanice pak má možnost toto SSID přijmout a použít jej pro přístup do sítě.

3.4 Shared-key autentizace

V případě použití této metody je nutno s síti používat také WEP. Každé zařízení s podporou šifrovaní WEP musí být schopno používat autentizaci sdíleného klíče.

Princip funkce spočívá v klíči, který je potřebný k přístupu do sítě. Takový klíč musí být známý každému zařízení, které chce do takové sítě přistupovat. Při požadavku o autentizaci se musí zařízení tímto klíčem prokázat, potom dojde ke kontrole ověření ze strany přístupového bodu. V případě, že se klíče shodují je zařízení v síti autentizováno. Samotný algoritmus ověření spočívá v tom, že klient odešle náhodné číslo, které je zakódované algoritmem RC4 podle daného klíče. Přístupový bod ho rozkóduje a pokud se klíče rovnají může dojít k autentizaci.

Při používání autentizace pomocí metody sdíleného klíče dochází k problému, že je nutné tyto klíče dost pravidelně měnit z důvodu rozšíření se i mezi neoprávněné osoby.



Obr.6 Autentizace sdíleným klíčem WiFi (6)

3.5 Typy útoku na bezdrátovou síť

Většina útoků vzniká z principu fungování bezdrátové sítě, kde nelze definovat prostor pokrytý signálem, a tím pádem nejde zamezit pokusům o neoprávněný přístup cizím osobám.

Rozluštění klíče WEP (WEP Cracking)

Tento postup je založen na použití hrubé síly. K rozluštění je potřeba mezi 5-10 miliony paketů, přičemž je podmínkou, že nedojde ke změně WEP klíče. Na internetu jsou k nalezení programy aircrack-ng a airsnor, které nabízejí tuto možnost.

Zjištění MAC adresy - MAC adresa pro připojení do sítě se dá odhalit úplně stejně jako se dá odhalit WEP klíč. Pokud není aktivována WEP, stačí útočníkovi zachytávat a procházet pakety, odhalit hlavičku MAC adresy a tu si pak přečíst. Pokud je použita WEP, nejprve musí útočník prolomit WEP a teprve potom může začít zkoumat přenos paketů. V okamžiku, kdy uživatel získá MAC adresu, může ji potom přenastavit na své kartě (pokud to karta umožňuje).

Man-in-the-Middle Atacks - Osoba, která chce dosáhnout neoprávněného přístupu vstoupí mezi přístupový bod a klienta. Přeruší veškerý provoz mezi nimi. Hacker zachytává provoz mezi AP a klientem během asociačního procesu. Tím získá základní informace o klientovi i AP. Pomocí těchto údajů potom vytvoří podvržený přístupový bod. Data od klienta zachytává na podvržený přístupový bod a dále přeposílá na původní přístupový bod.

Denial of Service(DoS) - jedná se o metodu, jejichž cílem je vyřazení sítě z provozu. Útočník zahltí přístupový bod velkým množstvím dat. Přístupový bod se snaží data vyhodnotit a přitom dojde k jeho přetížení, zahlcení a výpadku.

3.6 Bezpečnost v praxi

V této kapitole jsou shrnuty jednotlivé technické parametry do přehledných tabulek, které zobrazují výhody a nevýhody jednotlivých zabezpečení.

Tabulka č.4 Specifikace použitých zabezpečení (4)

	WEP	**WPA**	**802.11i(WPA2)**
Autentizace	otevřená	EAP-TLS PEAP	EAP-TLS PEAP
Šifrování	Statické WEP	TKIP/CKIP	AES

Tabulka č.5 Odolnost proti útoku (5)

Útok	**Odolnost**		
	WEP	**WPA**	**802.11i(WPA2)**
Integrita dat	dobrá	lepší	nejlepší
Falešná autentizace	špatná	nejlepší	nejlepší
Na slabý klíč	špatná	nejlepší	nejlepší
Falešný přístupový bod	minimální	lepší	lepší

Tabulka č.6 Vhodnost nasazení (6)

	Autentizace	**Šifrování**	**Velká síť**	**Malá síť**
WEP	nulová	WEP	špatná	dobrá
WPA(PSK)	PSK	TKIP	špatná	nejlepší
WPA2(PSK)	PSK	AES-CCMP	špatná	nejlepší
WPA	802.1x	TKIP	dobrá	dobrá
WPA2	802.1x	AES-CCMP	nejlepší	dobrá

4 Síťové komponenty

4.1 Repeater (Opakovač)

Opakovač je prvek, který pracuje na fyzické úrovni vrstvového modelu sítě. Jeho hlavním úkolem je obnova signálu. Signál přijatý na jeden port je obnoven a odeslán dále k cíli.

Všechny části spojené opakovači tvoří jeden fyzicky sdílený kanál (jednu kolizní doménu). Některé opakovače mohou přenášet pakety z jednoho typu fyzického média na jiný.

V souvislosti s wifi komponentami chápeme opakovač jako zařízení, díky kterému můžeme provozovat bezdrátovou síť pomocí více přípojných bodů. Jednotlivé bezdrátové přípojné body jsou spolu propojeny, a tím vznikne fungující bezdrátová síť. Samotnou konektivitu takové bezdrátové sítě například do internetu poté můžeme řešit připojením například ethernetové přípojky do jednoho ze zařízení.

4.2 Bridge (Most)

Mosty pracují na linkové vrstvě. Most průběžně přijímá příchozí rámce z obou sítí, které spojuje. Podle údajů uložených v hlavičkách rámců, rozhoduje zda bude nebo nebude rámec odevzdán do druhé sítě.

Most každý jednotlivý rámec přijme do své vyrovnávací paměti a tam analyzuje jeho obsah, aby dokázal identifikovat odesilatele a adresáta, na základě toho se potom rozhodne, co s rámcem udělá.

Pokud je u WiFi zařízení implementován režim Bridge(most) - je takové zařízení schopné, pokud bude tento režim nastaven, propojit (spojit) dvě sítě, například dvě LAN sítě případně LAN síť a WLAN.

4.3 Switch (Přepínač)

Přepínač je aktivní síťový prvek propojující jednotlivé segmenty sítě.

Přepínač pracuje na linkové vrstvě. Vedle vyššího výkonu znamená použití přepínačů přínos i pro bezpečnost sítě, protože médium již není sdíleno a data se vysílají jen do rozhraní, jímž je připojen jejich adresát.

Hlavní funkcí přepínače je přeposílání rámců na základě informací uložených v přepínací tabulce. Přepínač si z příchozích rámců čte nejenom cílovou fyzickou adresu, určující kam se bude rámec přepínat, ale také zdrojovou adresu a tu si spolu s číslem portu zaznamená do své přepínací tabulky.

Přijde-li rámec na konkrétní port přepínač vyhledá záznam v tabulce a přepojí rámec na příslušný odpovídající port.

Pokud přepínač dostane k doručení rámec směřující na jemu dosud neznámou adresu, chová se jako Hub, to znamená, že rozešle rámec do všech ostatních rozhraní, přičemž je pravděpodobné, že oslovená stanice odpoví a přepínač se tak vzápětí dozví, kde se nachází.

4.4 Router (Směrovač)

Směrovače se používají na úrovni síťové vrstvy. Jejich hlavním úkolem je směrování paketů jednotlivými sítěmi ležícími na cestě mezi zdrojovou a cílovou sítí. Používají se na propojení LAN sítí, připojení LAN sítě k WAN a propojení částí sítí WAN. Směrovače oddělují jednotlivé podsítě a tak filtrují všesměrové pakety určené pro danou síť. Znalost struktury paketů také směrovače předurčuje k možnosti implementace bezpečnostních mechanizmů (firewall).

4.5 Gateway (Brána)

V souvislosti TCP/IP se termín brána (Gateway) používá jako obecné označení směrovače (Router).

V TCP/IP se předpokládá, že jednotlivé (dílčí) sítě jsou přepojené prostřednictvím uzlů nazývaných brány (Gateways).

Vzájemné propojení je přitom takové, že mezi libovolnými dvěmi sítěmi existuje vždy aspoň jedna cesta, která může

vést i přes víc jiných dílčích sítí, resp. procházet posloupnost bran, které propojují mezilehlé sítě. Každá brána je připojená nejméně do dvou dílčích sítí a používá se pro směrování.

4.6 Access Point (Přístupový bod)

Access point (bezdrátový přístupový bod) je zařízení, které komunikuje s dalšími bezdrátovými zařízeními ve svém dosahu a stará se o směrování (routování) provozu mezi jednotlivými wifi klienty, případně mezi wifi klienty a pevnou (kabelovou sítí).

Toto uspořádání umožňuje komunikaci klientů připojených ke stejnému přístupovému bodu, aniž by byla nutná možnost přenášet signál přímo mezi klienty. Ve většině případů má ale i konektory RJ 45 do běžného ethernetu, a proto může sloužit například i jako jednoduchý router. Připojením bezdrátových zařízení jednotlivých klientů k přístupovému bodu vzniká bezdrátová síť.

4.7 Client (Klient)

Pod pojmem klient je chápána pracovní stanice (klasický stolní počítač, notebook, PDA), které využívá poskytovaných služeb prostřednictvím sítě. Tyto služby poskytuje v tomto případě přístupový bod (Access point). Klient jako takový musí byt vybaven síťovou kartou. U bezdrátových sítí je potřeba bezdrátová síťová karta, pomocí které se klient připojí k požadovanému přístupovému bodu.

5 Návrh síťové topologie

5.1 Současná situace

Firma HPh s.r.o. se rozhodla, že se přestěhuje z prostor, které již nedostačují současné výrobě, do nově zrekonstruovaných prostor. Firma se zabývá projekcí a sériovou výrobou dílů pro stavební stroje.

Na zakoupeném pozemku firmy se nacházejí dva objekty. První je dvoupodlažní budova, ve které bude umístěna veškerá administrativa firmy, vedení podniku plus projekční oddělení.

Druhým objektem je tovární hala, která bude upravena podle potřeb firmy. Součástí výrobní haly je i sklad polotovarů, hotových výrobků a expedice, která je odpovědná za distribuci a dopravu výrobků.

5.2 Počáteční rozvaha

Vedením podniku byla předložena zevrubná představa, jak by si představovala funkci nové vnitropodnikové sítě. V bodech se jedná:

- Provedení kompletního zasíťování kanceláří pro potřeby administrativy a běhu celé firmy
- Požadavek na případnou budoucí rozšiřitelnost
- Dostatečná rezerva propustnosti sítě
- Zabezpečení a garance kvality provozu

Ohledně použitých technologií pro samotnou realizaci počítačové sítě byla ponechána volnost rozhodování.

Budoucí síť by měla mít následující parametry

- Síť bude prozatím obsahovat okolo 25 počítačů.
- Vzájemné spojení části sítí v jednotlivých budovách bude realizováno pomocí bezdrátových spojů za použití standardu 802.11a a 802.11b.

- Použití dostatečně dimenzovaných zařízení umožní v budoucnu rozšířit síť podle potřeb - (Páteřní síť v administrativní budově bude řešena pomocí standardu IEEE 802.3ab).
- Pro bezpečnost provozu, lepší možnosti spravování a budoucího zvýšení výkonu celé sítě bude v síti použity vhodné mechanismy.

5.3 Typ sítě

Při rozhodování o typu sítě bylo rozhodnuto, že to bude síť typu klient/server. Tento typ sítě má výhodu v tom, že prostředky jsou centralizované na klíčových počítačích – serverech, které jsou stále v provozu a tím pádem pořád k dispozici. Další výhodou je škálovatelnost – servery je možné aktualizovat a případně v budoucnu doplnit dalšími v případě potřeby.

5.4 Technologie a architektura

V návrhu jsou použité klasické a ověřené technologie. V budovách je výhodné použít sítě Ethernet 1000BaseT, respektive Ethernet 100BaseT. V případě 100BaseT je použita kabeláž kategorie Cat-5e, u 1000BaseT kabeláž kategorie Cat-6.

Z důvodů požadavku na mobilitu a co nejmenší náklady na implementaci je návrh vhodně doplněn i o bezdrátové technologie standardu 801.11a a 802.11b pro spojení mezi administrativní budovou a přidruženými pracovišti na výrobní hale.

5.5 Organizační schéma oddělení

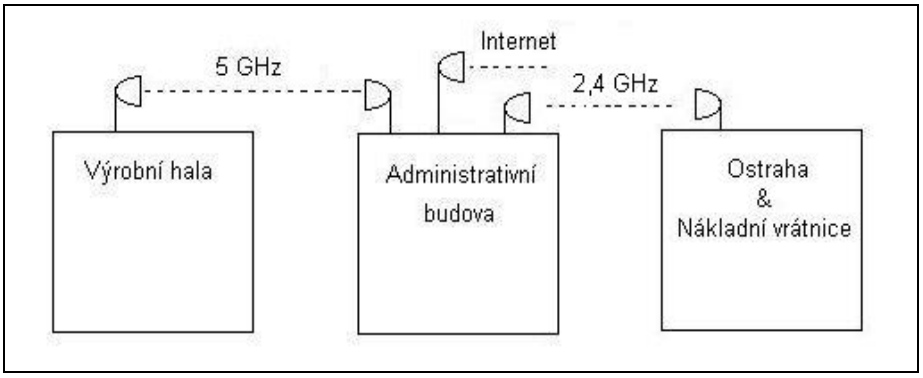
V administrativní budově jsou následující oddělení – obchodní oddělení, ekonomické (účetní, personální, marketingové) oddělení, vývojové oddělení, IT, ředitelství a vrátnice.

Ve výrobní hale jsou umístěny kromě samotné výroby ještě sklad, technologické oddělení, kancelář techniků a expedice hotových výrobků.

5.6 Schéma použití páteřních bezdrátových spojů

Propojení budov bezdrátovým spojením bylo zvoleno z důvodu, že plochy v okolí budov jsou pokryty asfaltem a náklady, které by vznikly případným propojením budov pomocí optických kabelů společně s výkopovými pracemi by byly podstatně větší než použití bezdrátového spojení.

Přenosová kapacita takového spoje při použití standardu 802.11a je reálně okolo 25 Mbit/s, což pro samotný provoz sítě stačí. Způsob konkrétní realizace bude popsán dále. Konektivita do internetu je také řešená bezdrátově s použitím technologie 802.11a s připojení do sítě některého z místních poskytovatelů internetu.



Obr.7 Schéma propojení budov mezi sebou

5.7 Realizace páteřního spoje 5 GHz

Intranetová síť v hlavní budově a výrobní hale bude spojovat dvojice bezdrátových zařízení pomocí standardu 802.11a pracující v pásmu 5 Ghz. Vzájemná komunikace bude v režimu AP (přístupový bod) a Klient. Tento režim nabízí vyšší datovou propustnost a menší zatížení, než režimu Bridge, který by se na první pohled mohl zdát jako nejvhodnější řešení.

Spoj realizovaný pomocí 802.11b není vhodný z důvodů malé přenosové rychlosti teoreticky 11 mbit/s, která neodpovídá požadavkům na propustnost sítě a zcela jistě by byla úzkým mís-

tem, které by způsobovalo problémy, stejně jako zabezpečení přenosu, které je u 802.11b pouze WEP. Toto zabezpečení již dnes nevyhovuje z důvodu snadného rozšifrování. Použití 802.11g sice nabízí vyšší rychlosti, ovšem v pásmu 2,4 GHz, které je v dnešní době již dost silně rušeno provozem ostatních zařízení pracující na stejné frekvenci. Proto se jako nejvhodnější řešení jeví použití technologie 802.11a pracující v pásmu 5 GHz, které je méně náchylné na rušení a zároveň není ve zdejších podmínkách tolik používané.

Pro samotnou realizace bezdrátového spoje je možné si vybrat z poměrně velkého počtu produktů. Nejvýhodnější řešením je použití embedded zařízení. Součástí takového zařízení je CPU, síťové karty, sloty mini-PCI, které lze osadit bezdrátovými kartami.

Použití tohoto zařízení osazeného vhodnými kartami vznikne spolehlivý a poměrně výkonný router (při zachování rozumné velikosti sítě), použitelný jak pro bezdrátovou síť tak pro LAN sít, případně kombinací obou. Toto zařízení nezabere mnoho místa, má minimální spotřebu a vysokou spolehlivost.

Na českém trhu je v nabídce několik takových zařízení od různých výrobců. Jedním z nich je RouterBoard.

Technické parametry RouterBoard [1] :

Procesor MIPS 175 MHz

Paměť 32 MB SDRAM

Ethernet:1-4x LAN auto MDI/X 10/100M

- 1xRS-232,1x PC Speaker, 1x konektor pro větrák
- 1-3x miniPCI slot
- 64MB NAND flash paměť s předinstalovaným OS
- napájení: JACK (11-60V), PoE (12-48V)
- pracovní provozní teplota: -20°C to +70°C

[1] http://www.routerboard.com/RB112.html

Použití Routerboardu je výhodné, protože nabízí vyšší výkon, než konkurenční zařízení. Jako software se používá routovací operační systém MikroTik. Ten disponuje velkým množstvím nastavení, díky němuž může toto zařízení fungovat jako bezdrátový AP, router, hardwarový firewall.

MikroTik je založen na OS Linux přičemž existují varianty jak pro klasické počítače, tak pro jednoúčelové zařízení (RouterBoardy).

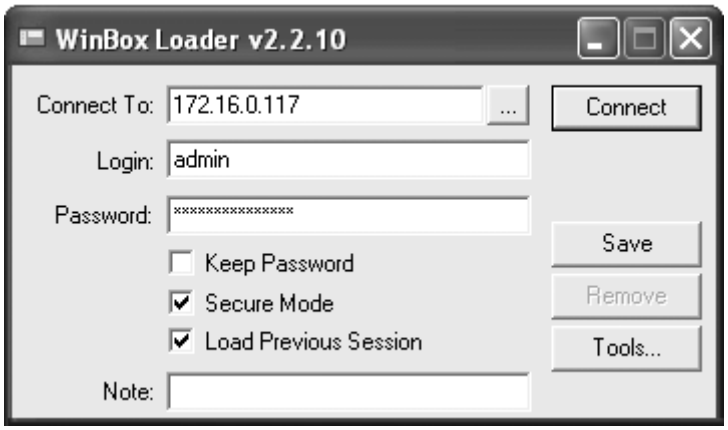
Pro spoj bude použit RouterBoard RB112/L4 jehož součásti je licence na používání OS MikroTik. Do slotu mini-PCI je osazena bezdrátová karta Atheros AR5413. Tato karta podporuje standard 802.11a.

Obr.8 RouterBoard RB112 (7)

Konfigurace a přístup do zařízení je možný přes sériové rozhraní nebo přes konzoly.

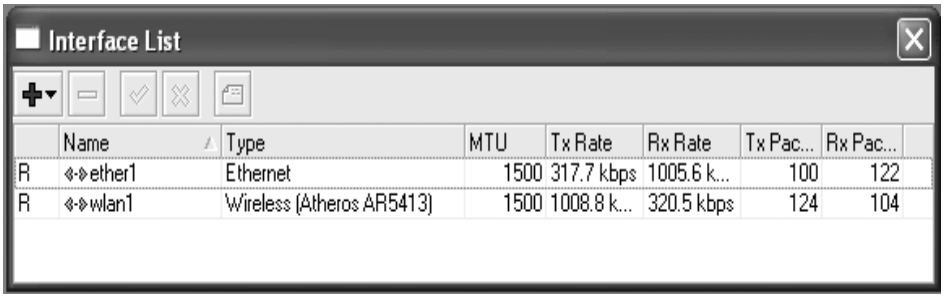
Pro prvotní nastavení je nutné použít příkazovou řádku, pomocí které se nastaví IP adresa zařízení a síťové rozhraní, přes které bude možné přistupovat při další konfiguraci.

Po této úvodní konfiguraci můžeme použít utilitu WinBox, která nám umožní přihlášení k MikroTiku.



Obr.9 Utilita WinBox

Po přihlášení do MikroTiku je ve složce Interfaces vidět výpis rozhraní zařízení. V tomto případě se jedná o Routerboard, který má pouze jedno ethernetové rozhraní a jedno bezdrátové rozhraní.

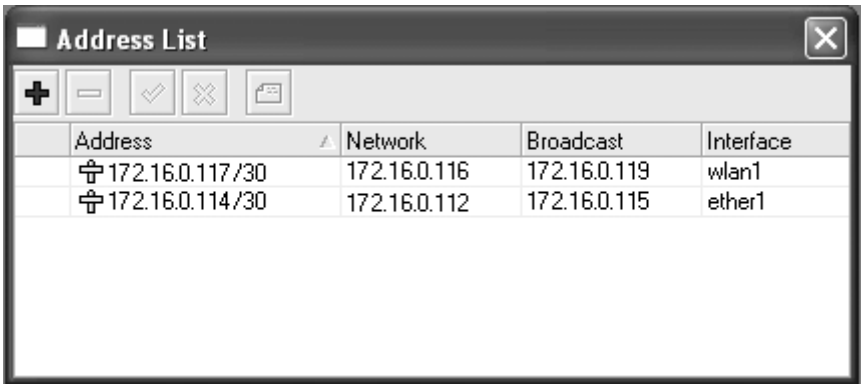


Obr.10 Výpis rozhraní

Rozhraním je nutné přiřadit IP adresy pro pozdější nastavení routování. MicroTik OS používá pro definici IP adres zkráceny zápis masky sítě.

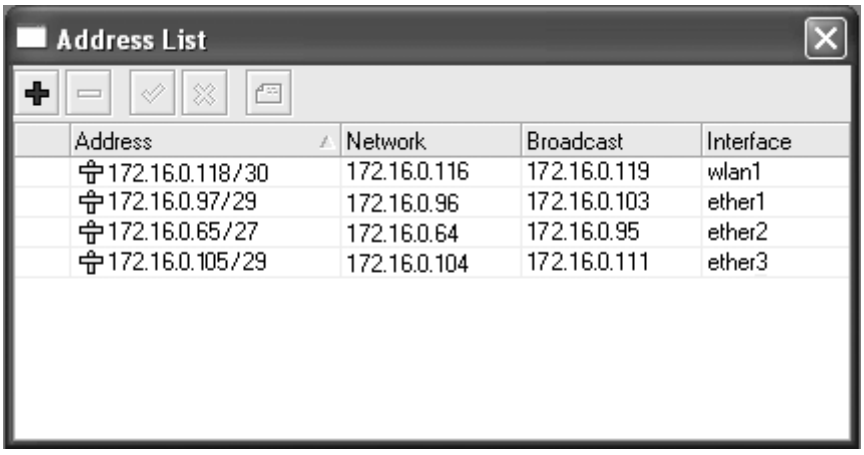
Nastavení síťových rozhraní

Podle zpracovaného návrhu byly pro jednotlivá rozhraní nastaveny potřebné IP adresy. Routerboard RB112 má jedno ethernetové rozhraní a jedno bezdrátové rozhraní WLAN osazené bezdrátovou kartou Atheros AR5413. Ether1 je nastaveno na 172.16.0.114/30 a wlan1 rozhraní je nastaveno na 172.16.0.117/30.



Obr.11 Nastavení rozhraní na Routerboard režim AP

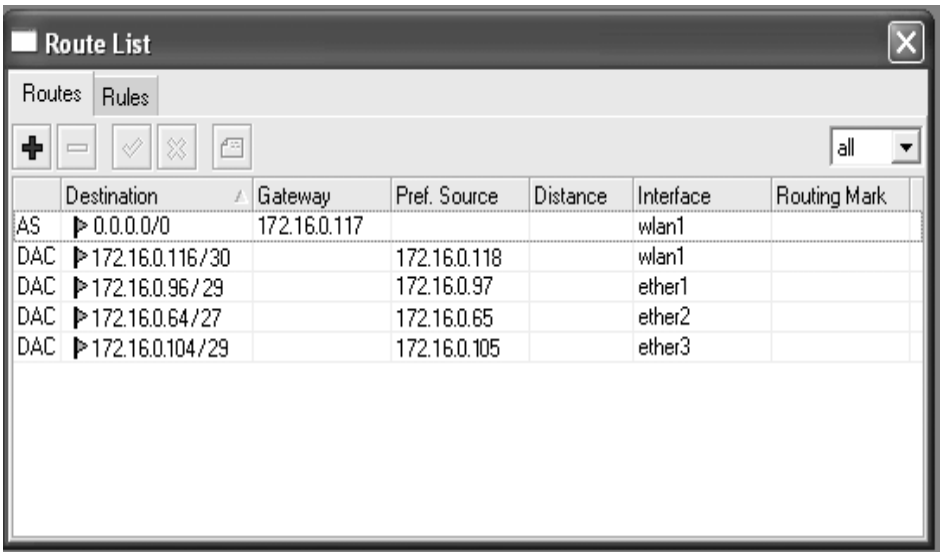
Rovněž na druhém zařízením je pro provoz potřeba nastavit IP adresy pro jednotlivá rozhraní. V tomto případě se jedná o zařízení routerboard RB 532A. Toto zařízení obsahuje 3 ethernetová rozhraní a 2 pozice s mini PCI sloty, přičemž v jednom ze slotu je osazena karta Atheros AR 5413.



Obr.12 Nastavení rozhraní na Routerboard režim Klient

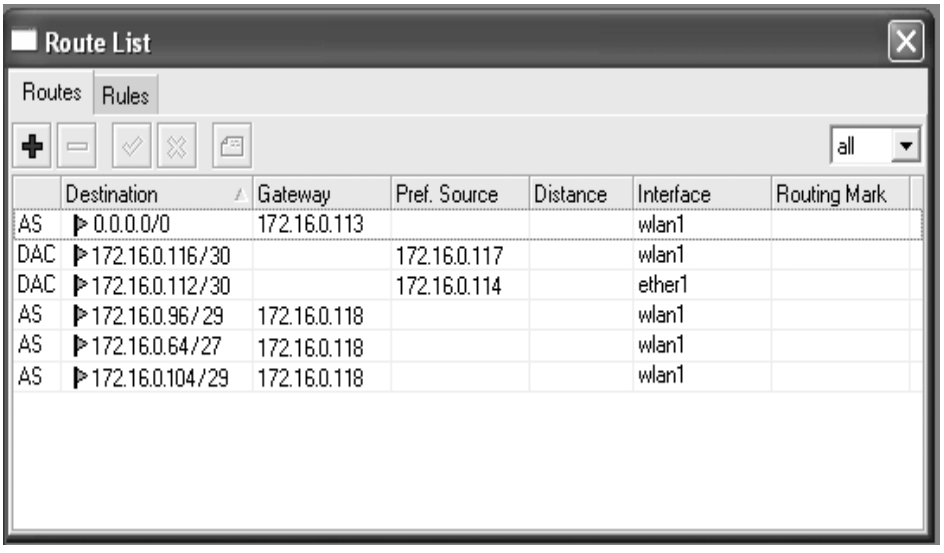
Nastavení Routování

Pro provoz zařízení (routerboard v režimu klient na střeše výrobní haly) je nutné doplnit údaje do routovací tabulky. Jako defaultní gateway pro wlan1 je nastavena IP adresa 172.16.117, což je IP adresa bezdrátové karty na druhé straně spoje. Ostatní routovací údaje v tabulce definuji na které rozhraní, odpovídající dané podsíti, mají být posílány příchozí pakety.



Obr.13 Routovací tabulka na Routerboard1

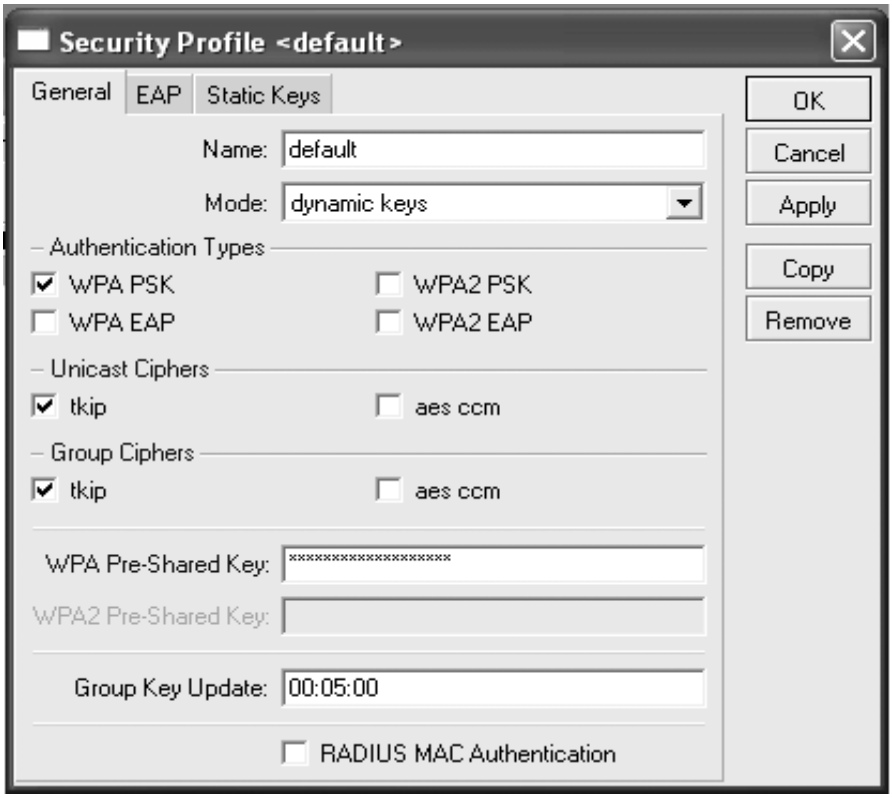
I druhé zařízení routerboard pro svůj provoz potřebuje nastavit routovací tabulku. Defaultní gateway pro je nastavena na 172.16.0.114, což je síťové rozhraní v routeboardu. Další směrovací údaje jsou uvedeny v obrázku číslo 16 viz. níže.



Obr.14 Routovací tabulka na Routerboard 2

Nastavení zabezpečení bezdrátových karet Atheros AR 5413

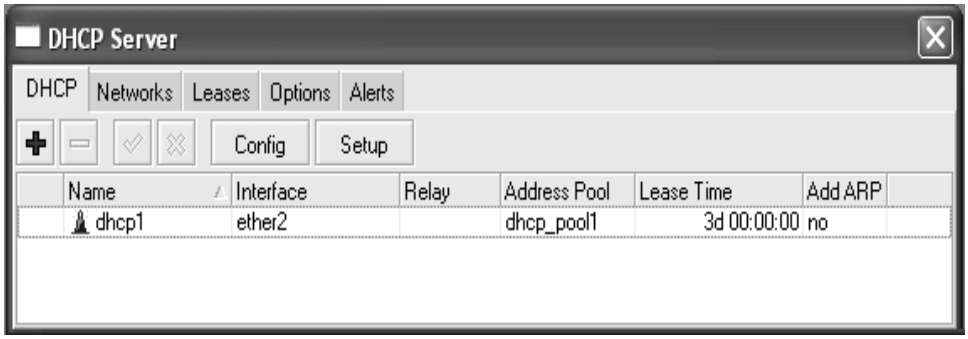
Security profil je nechám na default, přenos je zabezpečen pomocí WPA se sdíleným klíčem.



Obr.15 Nastavení zabezpečení

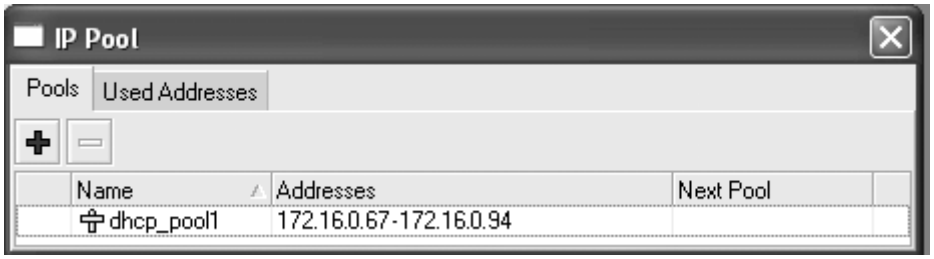
Nastaveni DHCP

Stanicím v síti 172.16.0.64/27 (výrobní hala) budou přidělovány IP adresy dynamicky pomocí DHCP. Server poběží na Routerboardu pro rozhraní ether2, do kterého je připojena síť 172.16.0.64/27.



Obr.16 DHCP server

Rozsah přidělovaných adres se nastaví v menu IP – Pool. Rozsah je zde nastaven na rozsah 172.16.0.67-172.16.0.94.



Obr.17 Nastavení rozsahu přidělovaných adres

5.8 Nastavení bezdrátových prvků 2,4 GHz

5.8.1 Bezdrátový spoj - hlavní budova vrátnice

Tento bezdrátový spoj umožňuje připojení dvou počítačů, které se nacházejí v prostoru nákladní vrátnice do podnikové sítě. Počítače zde umístěné bude používat obsluha vrátnice.

Z důvodu pouhých dvou počítačů se uvažovalo o tom, zda vůbec tyto počítače připojovat k sítí a nebo je nechat jako sólové počítače. Po konzultaci bylo rozhodnuto připojit i tyto počítače. Připojení je realizováno pomocí dvou zařízení OvisLink WL-5460AP.

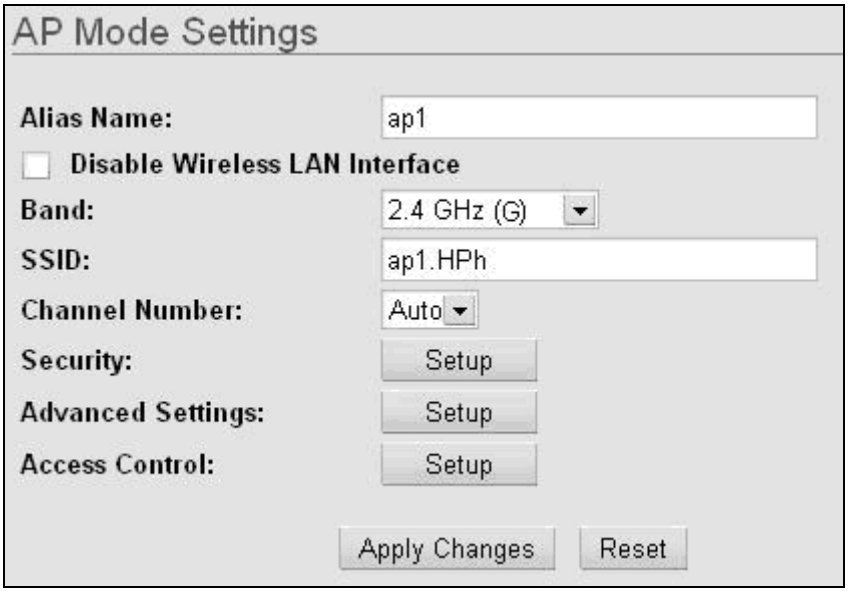
Jeden bude v nastavení Access Point a druhý v režimu Klient. Diky tomu, že toto zařízení obsahuje dvouportový switch, není pro připojení počítačů na vrátnici potřeba již žádný další aktivní síťový prvek.

Ovislink budu pomocí kroucené dvoulinky přímo připojen na síťový adaptér v hlavním serveru.. Pro venkovní použití na menší vzdálenost se hodí PAN-10 anténa. Je to sektorová anténa pro venkovní použití určená pro pásmo 2,4 GHz.

Obr.18 Sektorová anténa PAN-10 (8)

Nastavení do režimu AP

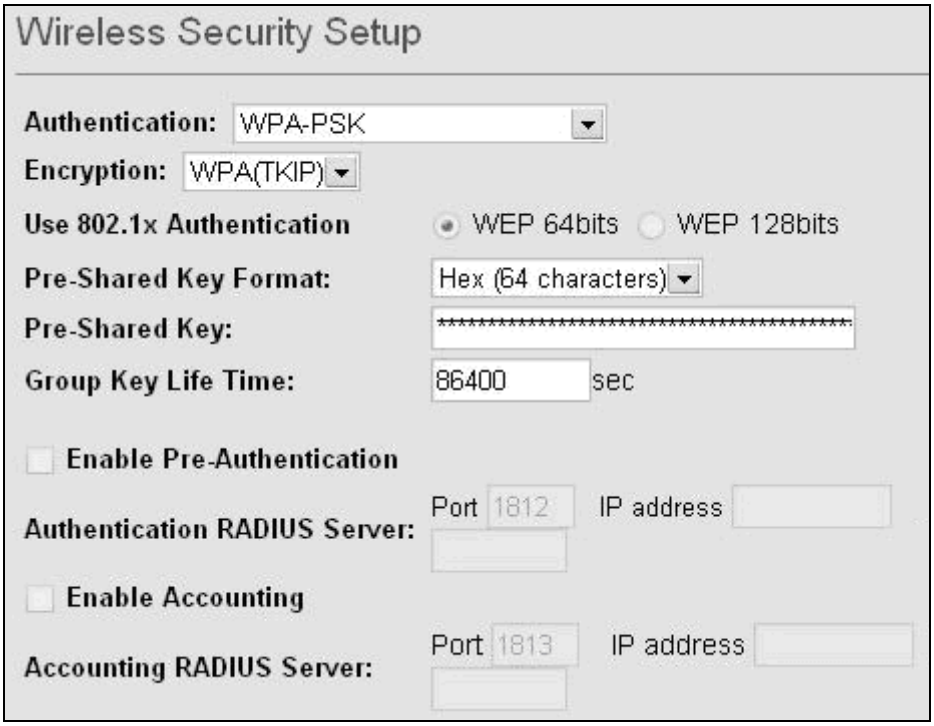
Nastavit zařízení do režimu AP není nijak náročné. Nastavení se provádí pomocí webového rozhraní. Defaultní tovární IP adresa zařízení je 192.168.100.252.



Obr.19 Základní nastaveni zařízení Ovislink režim AP

Volba kanálu je nastaveno na auto. Samotný provoz je nastaven v 802.11g.

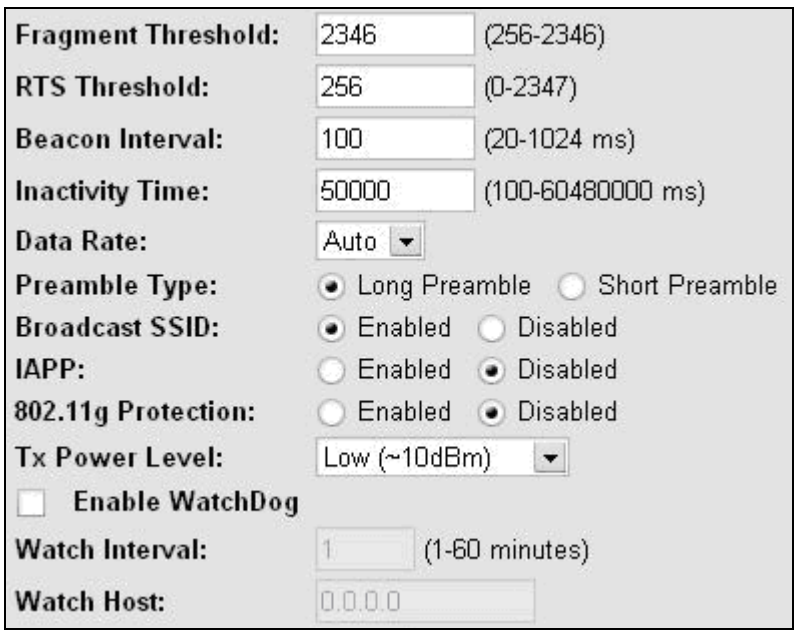
Nastavení zabezpečení



Obr.20 Zabezpečení zařízení Ovislink režim AP

Zabezpečení je nastaveno na WPA se sdíleným klíčem. Kódování na WPA (TKIP). V síti není použit autentifikační server RADIUS a proto zůstanou příslušné volby neaktivní.

Rozšířené nastavení



Obr.21 Nastavení WLAN části - Ovislink režimu AP

Fragment Treshold byl ponechán na maximální hodnotu. Tato vlastnost se používá pro fragmentaci paketů, což napomáhá zlepšení výkonu v případě rušení rádiovou frekvencí.

RTS Treshold udává velikosti paketu. Od této velikosti se začíná používat přenosový protokol RTS/CTS na místo běžného CSMA/CA. CSMA/CA pracuje na principu, kdy klient naslouchá na své frekvenci a vysílá, když žádný jiný klient nevysílá. Při venkovním použití o sobě klienti nevědí, a proto všichni vysílají, zahlcují pásmo, navzájem se ruší a dochází ke ztrátám paketů.

Alternativní protokol je RTS/CTS, kdy klient nejdřív požádá o vysílání, dostane od AP povolení na určitou dobu a začne vysílat, ostatní klienti po stanovenou dobu mlčí. Aby toto nastavení fungovalo, musí být nastaveno na všech zařízeních stejná hodnota. V praxi se osvědčila pro přepnutí na RTS/CTS nastavit spodní velikost paketu na 256 bytů.

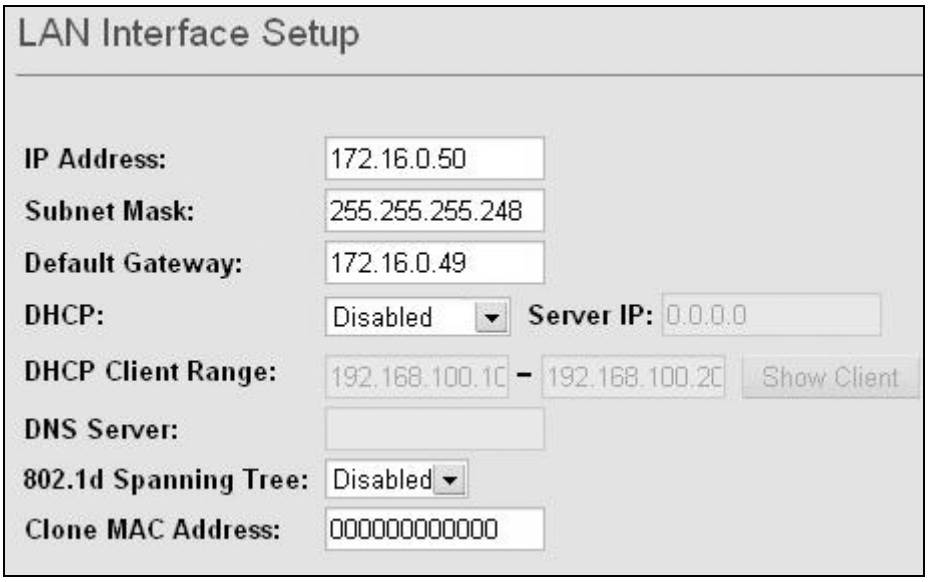
Nastavení je ponecháno na tovární hodnotě. Při experimentování s touto hodnotou nebyly pozorovány žádné změny při přenosu. Beacon Interval vysílá každé bezdrátové zařízení. Při vysílání se zařízení přepne do předem definované modulace (dle specifikace WiFi), což je: 802.11b = 2 Mbis/s 802.11g = 6 Mbit/s.

Volba Data Rate definuje rychlost přenosu. V tomto případě byla nastavena na rychlost 11 Mbit/s, což po odečtení režie na přenos představuje rychlost okolo 6 Mbit/s. Preambule Type ovlivňuje přenosovou rychlost. V případě Long Preamble je tento začátek paketu vysílán na 1 Mbit/s, stejně jako hlavička paketu, celý tento proces trvá 192ms a praktická propustnost 802.11b nepřekročí 5,5 Mbit/s datového toku. Nastavení Short Preambule, které zkracuje počáteční synchronizaci paketu tak, že Preamble se sice pořád vysílá na 1 Mbit/s, ale hlavička již na 2 Mbit/s a to zkracuje čas pro odeslání těchto synchronizačních a hlavičkových dat na 96ms.

TX Power Level definuje sílu vysílacího výkonu. Zde je důležité dodržovat nařízení podle normy - maximální vysílací výkon v České Republice je 100mW. Nastaveno je Low. V kombinaci

s anténou a délkou kabelu je výkon dostačující bezproblémovému provozu.

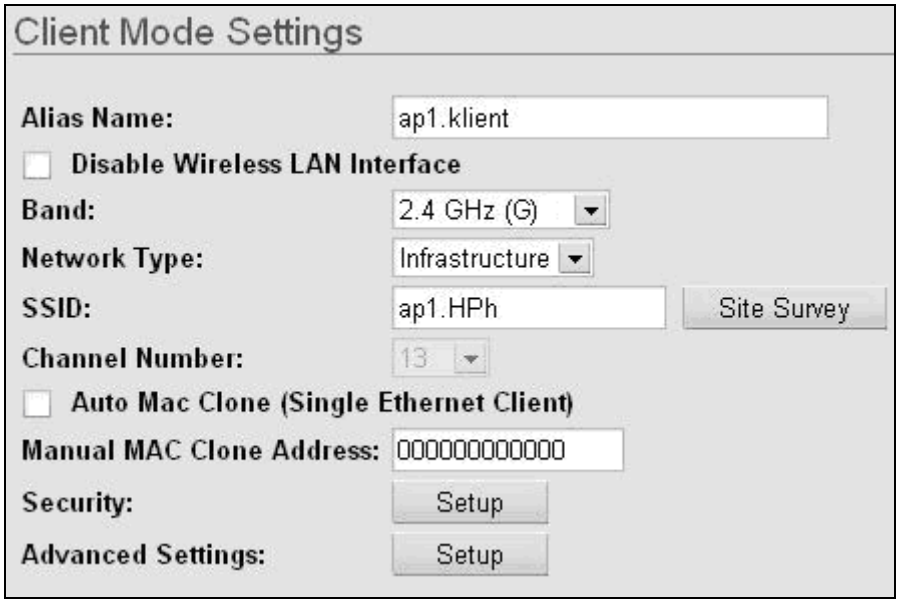
Nastavení LAN Rozhraní



Obr.22 Nastavení LAN části - Ovislink režimu AP

IP address je nastavena podle návrhu na 172.16.0.51, maska na 255.255.255.248. Gateway v tomto případě bude IP adresa 172.16.0.50 síťové karty v hlavním server. DHCP server je vypnut. Koncové počítače budou mít nastaveny statické IP adresy.

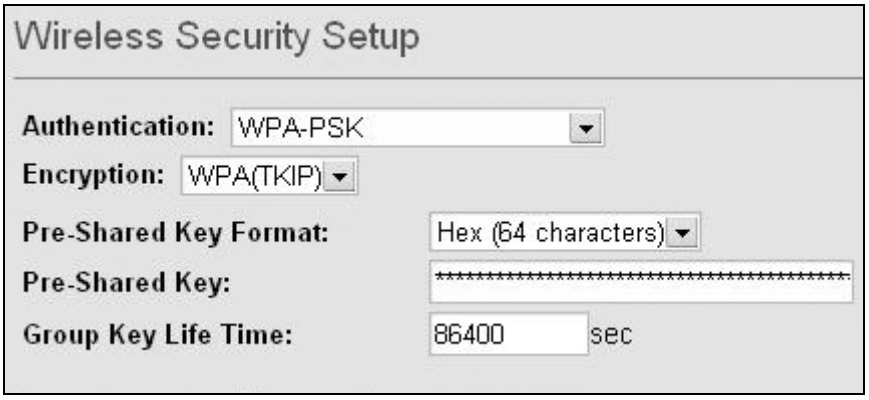
Nastaveni do režimu klient



Obr.23 Základní nastavení - Ovislink režim klient

Přenos je nastaven na standard 802.11g stejně jako přístupový bod. Typ sítě je nastaven na Infrastructure tedy komunikace prostřednictvím přístupového bodu. SSID je nastaveno podle přístupového bodu na ap1.HPh. Kanál je zařízením vybrán automaticky podle přístupového bodu.

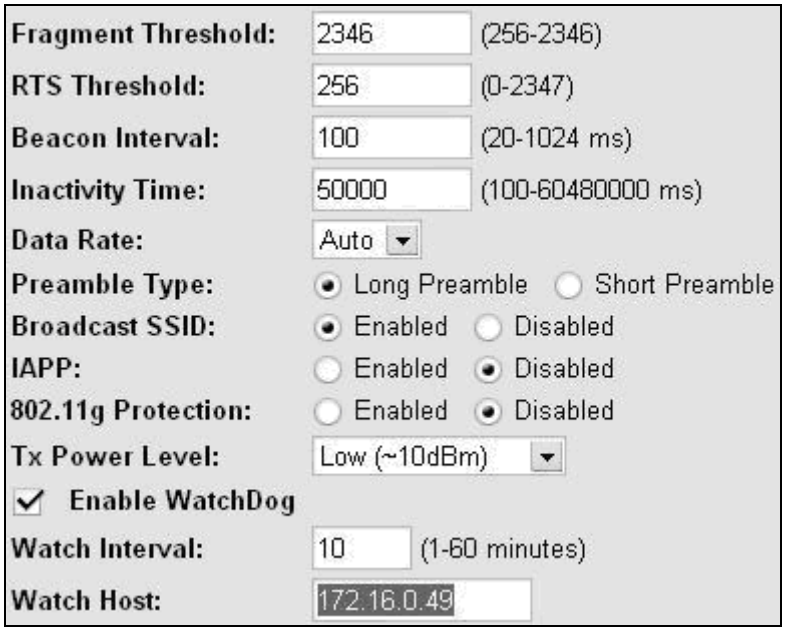
Zabezpečení



Obr.25 Zabezpečení - Ovislink režim klient

Autentifikace je pomocí WPA-PSK. Šifrování je nastaveno na WPA, které poskytuje podstatně lepší ochranu než použití WEP. Dále je zde nastavena Formát sdíleného klíče a samotný klíč, bez kterého by se nemohl klient připojit k přístupovému bodu. Ostatní nastavení zůstalo tak jak bylo.

Rozšířené nastavení



Obr.24 Základní nastavení - Ovislink režim klient

Nastavení je zde prakticky identické jako na přístupovém bodě. Fragment Threshold je nechán přednastaven, RTS Treshold je nastaveno na 256 Bytů, Beacon Interval a Inactivity Time je necháno na původním nastavení. Preambule Type je nastaven na Long Type. IAPP a 802.11g je vypnuto. Vysílací výkon je nastaven na Low.

WatchDog je zapnut. Po zkušenost se jako optimální doba mezi intervaly doporučuje 10 minut.

Nastavení LAN Rozhraní

Podle návrhu byly přiřazena IP adresa 172.16.0.52 podmaska 255.255.255.248. Gateway je nastavena na 172.16.0.49. DHCP server není zapnut. IP adresy na počítačích jsou nastaveny staticky.

5.8.2 Přístupové body uvnitř budov

V návrhu sítí je použito několik přístupových bodu. Jeden je použit ve skladu ve výrobní hale, druhý je použit v oddělení expedice a třetí je použit v administrativní budově. U všech je počítáno, že budou pracovat v pásmu 2,4 GHz. Při jejich provozu se nepočítá s tím, že by byly nějak výrazně vytíženy, jsou zde spíše umístěny proto, aby zaměstnancům v oddělení expedice a skladu umožnily efektivnější a snadnější práci. Zde by měly plnit funkci především v případech, kdy zaměstnanec se pohybuje v prostoru skladu a může pomocí přenosných zařízení provádět kontrolu stavu výrobků a rovnou pracovat bez nutnosti se vracet k pracovní stanici, která je připojena k ethernetu. Stejně tak tomu je v případě expedice, kde možnost případného okamžitého přístupu na síť měla vést k ulehčení práce pracovníkům a k vyšší efektivitě.

Přístupový bod v administrativní budově je umístěn v konferenční místnosti. Tento přístupový bod měl umožnit komunikaci mezi účastníky porad, jednání se zákazníky, různými návštěvami a podobně. Tyto osoby se k přístupovému bodu připojí

a mohou navzájem komunikovat, případně použít připojení k internetu.

Přístupový bod jako takový má svoje vlastní ethernetové připojení přímo do hlavního serveru. Tato varianta byla zvolena z důvodu bezpečnosti, aby bylo znemožněno nepověřeným osobám dostat se k vnitropodnikovým informacím a na vnitřní síť.

Díky nastavení na hlavním serveru (routeru) je možné vhodnými nástroji nastavit příslušná práva, které dovolí například zákazníkům maximálně připojení do internetu stejně jako možnost odeslat a přijmout email. Samozřejmě podle aktuální potřeby je možné toto nastavení zpřísňovat, případně povolit další nezbytně nutné porty, které pro svůj běh vyžaduje příslušná aplikace.

Obr.26 Ovislink WL-5460 (9)

Jako vhodné zařízení byl vybrán spolehlivý Ovislink WL-5460 AP. Výhodou je, že pro toto zařízení existuje speciální firmware, který přidá spoustu dalších funkcí a zvýší tak hodnotu toho to zařízení.

S továrním firmwarem nabízí následující parametry[2]:

- Módy: AP, Bridge, Client, WDS
- Standardy: 802.11b, 802.11g
- Bezpečnost: WEP, WPA, WPA 2

[2] http://www.czechcomputer.cz/product.jsp?artno=34039

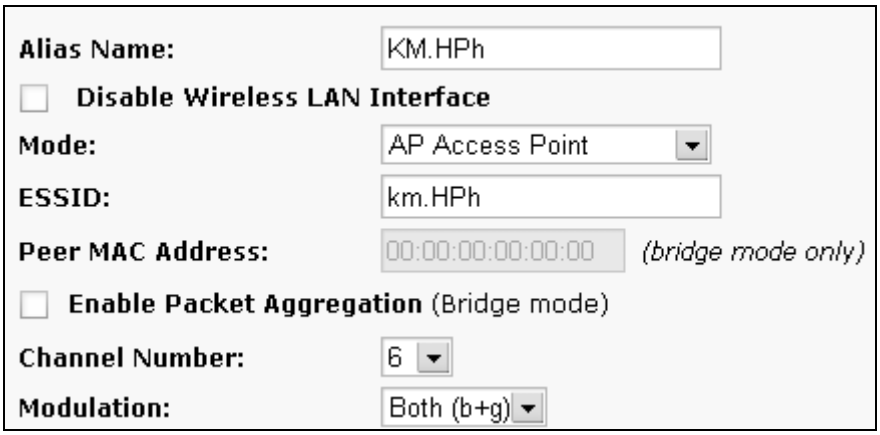
Po použití firmwaru APPro toto zařízení nabídne při zachování původních funkcí navíc[3]:

- Režim Infrastructure client, AdHoc client, Bridge Point to Point, Point to Multipoint, Secure WDS.
- Oddělené nastavení pro LAN 1 , LAN 2 a WLAN rozhraní, DHCP server
- Routování a omezování rychlosti mezi WLAN, LAN 1 a LAN 2 rozhraním, překlad adres NAT
- Klonování MAC adresy, omezování rychlosti
- Omezení přístupu na základě MAC adresy

5.8.3 Přístupový bod v konferenční místnosti

Přístupový bod v konferenční místnosti bude Ovislink WL-5460 s firmwarem APPro.

Nastavení do režimu AP

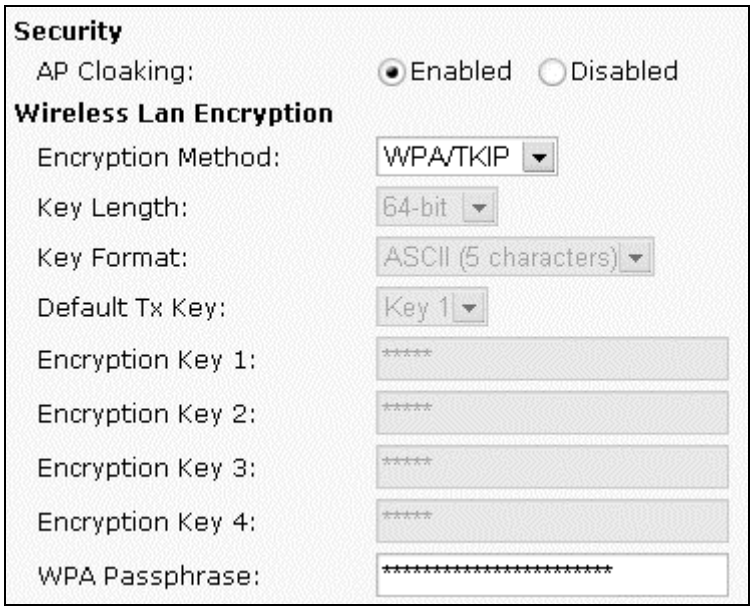


Obr.27 Základní nastavení

Název je nastaven na KM.HPh.(KM=Konferenční místnost). Zařízení je nastaveno na Access point (přístupový bod). ESSID je nastaveno na km.HPh. Při přenosu bude použit 6. kanál. Na přístupový bod bude možné se připojit se zařízení podporující jak 802.11b tak 802.11g.

[3] http://www.appro.cz/funkce.html

Zabezpečení



Obr.28 Nastavení šifrování

Zabezpečení je nastaveno na WPA/TKIP se sdíleným klíčem.Takové zabezpečení poskytuje dostatečnou ochranu proti případným pokusům o průnik do sítě

Rozšířené nastavení

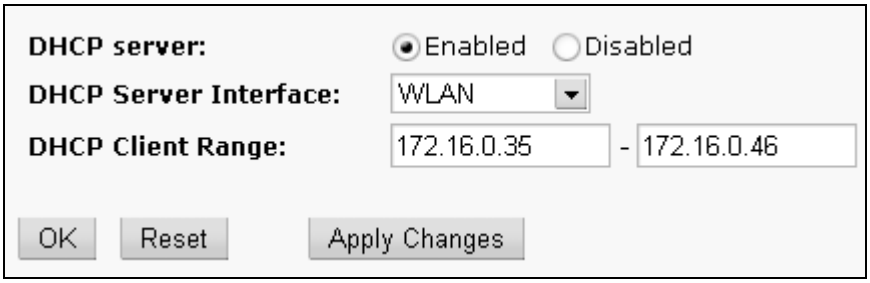
Fragment Treshold je nastaven na default hodnotu. RTS Treshold je nastaven na 256 Bytů,.

Vysílací výkon je nastaven na nejnižší možný výkon, aby pokrytí signálem co nejméně přesahovalo prostory místnosti.

Rychlost je nastavena na „auto“ to znamená, že rychlost se mění podle aktuálního stavu.

Dále je zapnuto blokování IBSS traffic jehož přínosem je izolace klientů. Důsledkem tohoto nastavení je, že klienti o sobě nevědí a nepředávají si mezi sebou servisní data, čímž zamezují zbytečnému přenosu.

Nastaveni DHCP



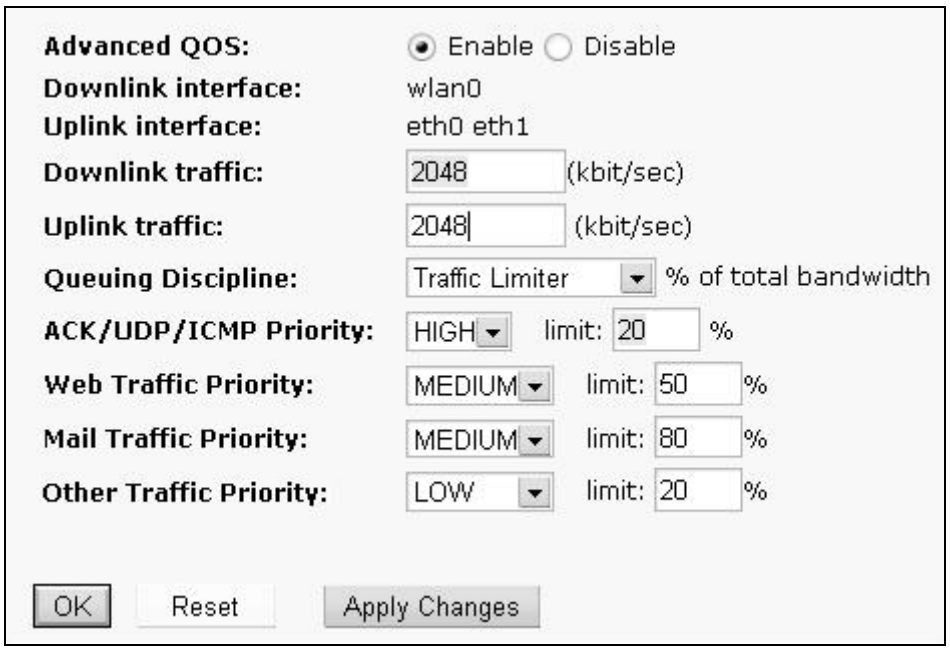
Obr.29 Nastaveni DHCP serveru

Na rozhraní WLAN poběží DHCP server, který bude přidělovat IP adresy v rozsahu 172.16.0.35 -172.16.0.46.

Nastavení LAN rozhraní

IP adresa je nastavena na 172.16.0.34, podsíť je 255.255.255.240, gateway je nastavena na 172.16.0.33. Režim na ethernetové části AP je nastaven na režim Bridge.

Nastavení QoS



Obr.30 Nastavení QoS

Quality of Service (QoS) – je řízení provozu v síti. Protokol zajišťuje rovnoměrné dělení celkového pásma mezi jednotlivé uživatele. Cílem je, aby nedocházelo k zahlcování sítě. Nejvyšší prio-

ritu mají servisní pakety, poté následuje webový přenos společně s maily. Nejnižší prioritu mají ostatní pakety.

5.8.4 Přístupové body v oddělení skladu a expedice

Tento přístupový bod je v tomto prostoru umístěn, aby ušetřil a zefektivnil práci v prostorech skladu a přilehlých prostorech haly. Z tohoto důvodu bude použita sektorová anténa, aby se co možná nejméně vysílaný signál přesahoval oblast plánovaného pokrytí signálem.

Důvod, proč je zde přístupový bod vůbec umístěn je ten, že zaměstnanci ve skladu mohou používat například PDA s podporou WiFi, a tím pádem se mohou pohybovat v prostorech a lépe plnit svou práci.

Praktické využití může takové zařízení nalézt i v případě různých kontroly skladových zásob nebo plánování logistického zabezpečení, kdy se pracovník může pohybovat mezi skladovými zásobami a prakticky okamžitě na PDA posílat potřebné údaje bez potřeby zbytečných poznámek, které by pak musel přepisovat na počítači v kanceláři.

Pro provoz v takové sítí je potřeba použít takové PDA, které podporuje standard 802.11g. Ještě donedávna nebylo použití standardu 802.11g možné, protože přenosná zařízení tento standard nepodporovala.

Toto je naštěstí dnes již vyřešeno, protože operační systém Windows Mobile 2005 již poskytuje podporu i pro standard 802.11g. Díky tomu je možné použít na přístupovém bodu zabezpečení pomocí WPA, čím se stane takový přenos v reálném čase neprolomitelný.

Jako zařízení bude opět použit Ovislink 5460 se speciálním firmwarem APPro.

Přístupový bod sklad

Zařízení bude mít nastaveno IP adresu 172.16.0.106, maska podsítě bude 255.255.255.248, což umožní teoretické připojení až 5 zařízení. Výchozí brána bude nastavena na 172.16.0.105.

Přístupový bod bude pojmenován sklad.HPh. Režim bude samozřejmě nastaven na Access point. SSID bude sklad.HPh

Přístupový bod expedice

Zařízení bude mít nastaveno IP adresu 172.16.0.98, maska podsítě bude 255.255.255.248, což umožní teoretické připojení až 5 zařízení. Výchozí brána bude nastavena na 172.16.0.97.

Přístupový bod bude pojmenován expedice.HPh. Režim bude samozřejmě nastaven na Access point. SSID bude sklad.HPh.

Nastavení společné pro oba přístupové body

Přístupové body budou nastaveny na provoz v 802.11g. Zabezpečení bude nastaveno na WPA(TKIP) se sdíleným klíčem.

Fragment Treshold zůstane nastaven na původním nastavení. RTS Treshold bude nastaven na 512. Preamble type je nastaven na long. Rychlost přenosu bude nastavena na 11mbit/s, což plně postačuje provozním potřebám. Ostatní parametry v rozšířeném nastavení WLAN jsou ponechány na původním nastavení. Na WLAN bude zapnut DHCP server s tím, že rozsah přidělovaných adres je nastaven na 3 možná zařízení, přestože velikost masky sítě umožňuje připojení více zařízení. Důvodem je skutečnost, že nastavený rozsah pro 3 zařízení plně postačuje potřebám oddělení a do budoucna není problém tento rozsah podle potřeby upravit.

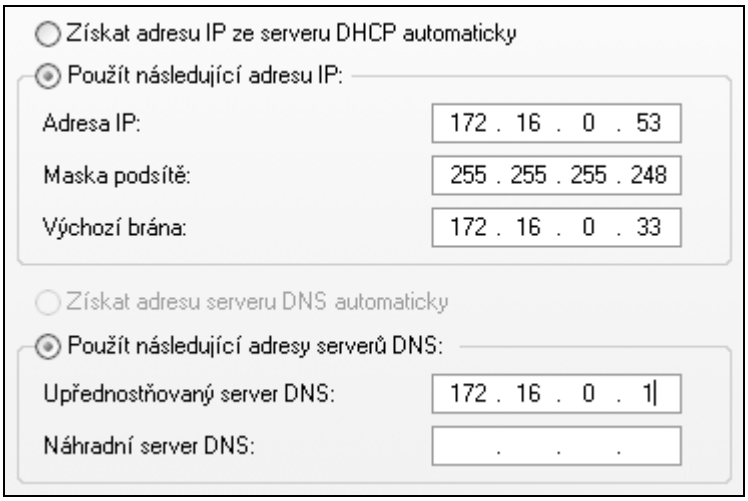
Z důvodu bezpečnosti bude zapnuta kontrola MAC adres zařízení, které se budou do sítě připojovat.

5.9 Nastavení pracovních stanic

Pro připojení do sítě je nutné nastavit pracovním stanicím IP adresu, masku podsítě, výchozí bránu a DNS server.

V tomto konkrétním případě se jedná o nastavení pracovní stanice v prostoru nákladní vrátnice.

Nastavení síťového rozhraní pracovní stanice



Obr.31 Nastaveni TCP/IP na pracovní stanici

5.10 Nastavení přepínačů

Navrhovaná síť se skládá z většího množství počítačů, a proto není vhodné použít nejlevnější přepínače. Kvůli bezpečnosti a odstranění zbytečné redundance v sítí je vhodné použít spravovatelné přepínače. Nabízejí některá pokročilá nastavení jako je VLAN(802.1Q), kontrola přenosu, prioritizace komunikace (802.1p).V návrhu jsem použil přepínače od firmy HP typ ProCurve1800. Tato řada se vyznačuje přepínatelnou rychlostí přenosu 10/1001000 Mbit/s se základními funkcemi pro správu a konfiguraci.

Obr.32 Switch HP ProCurve 1800-8G (10)

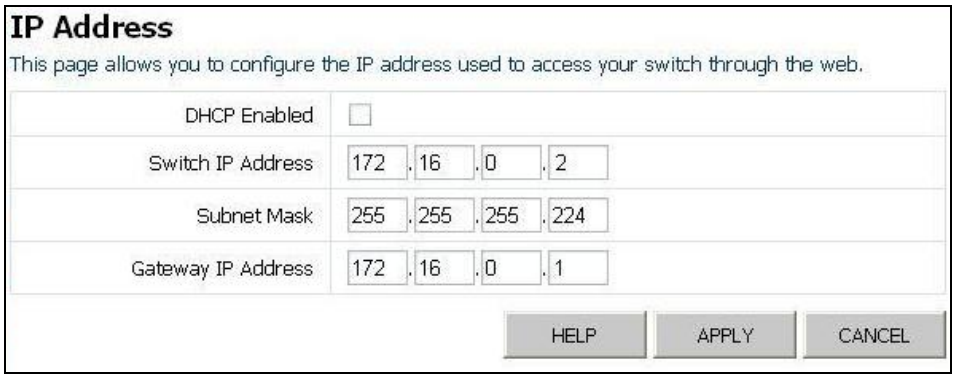
Technické parametry[4]

Ports: 8x 10/100/1000 ports (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab 1000Base-T)

[4] http://www.bgslevi.cz/produkt_detail.php?id=40739

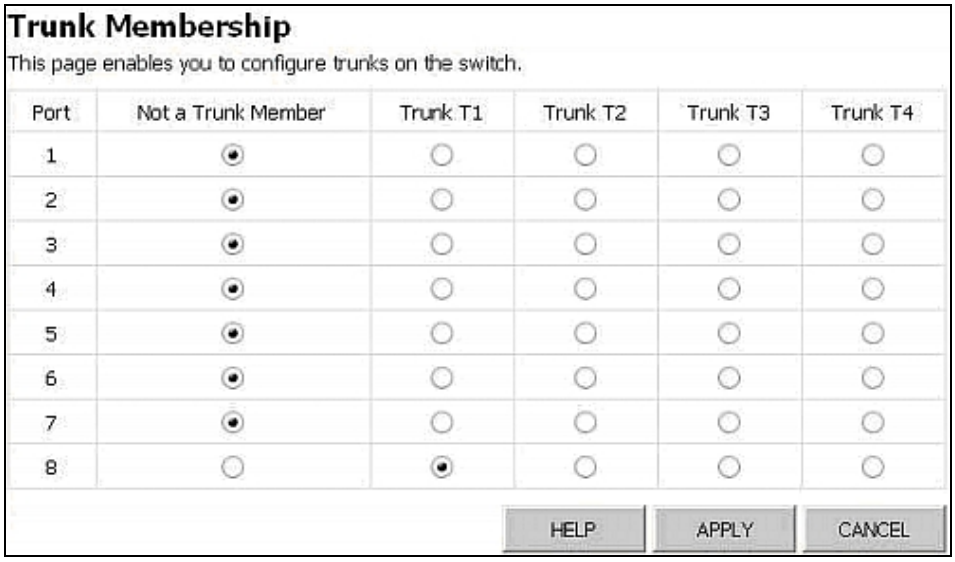
• RAM/ROM capacity: 2 MB, Flash capacity 2MB,SDRAM 64KB
• IEEE 802.3x Flow Control
• IEEE 802.3ad Link Aggregation Control Protocol
• IEEE 802.1AB Link Layer Discovery Protocol
• IEEE 802.1Q VLANs
• IEEE 802.1p Priority

V továrním nastavení je nutné nejprve na počítači nastavit 192.168.2.x masky 255.255.255.0. Default IP adresa přepínače je 192.168.2.10. Po nastavení do sítě bude mít následující nastavení.



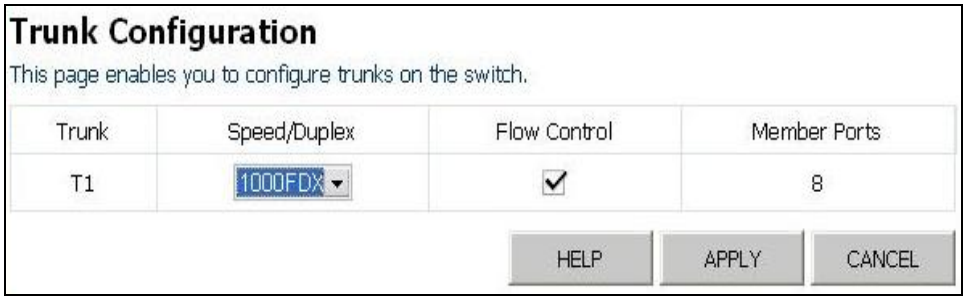
Obr.33 Nastavení IP adresy

Z důvodu přístupu přes webové rozhraní musí mít přepínač svoji vlastní IP adresu, aby bylo možné na něho vzdáleně přistupovat a spravovat a konfigurovat.



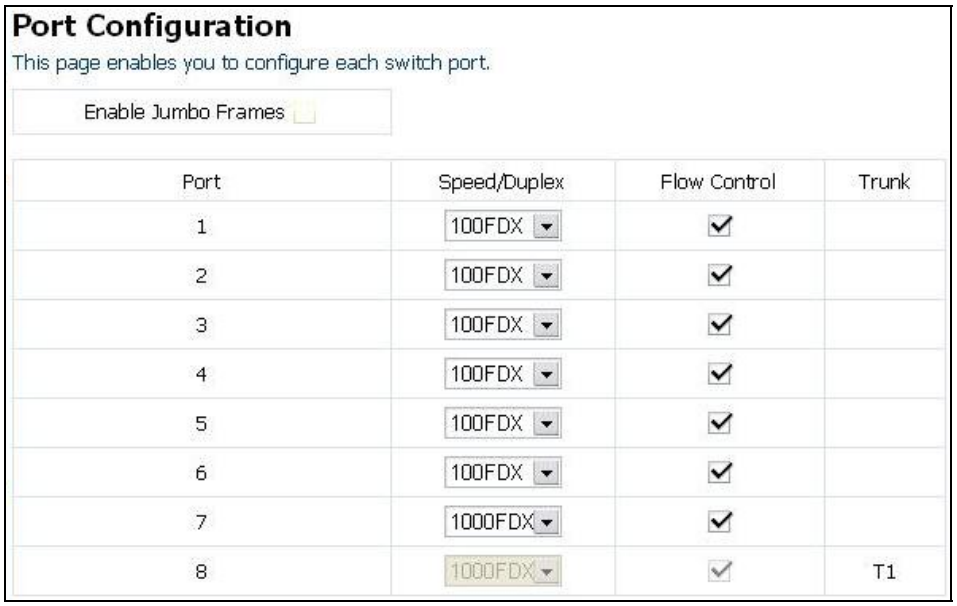
Obr.34 Nastavení Trunk

Port 8 je určen speciálně pro propojení s dalším switchem pomocí Trunku.



Obr.35 Trunk konfigurace

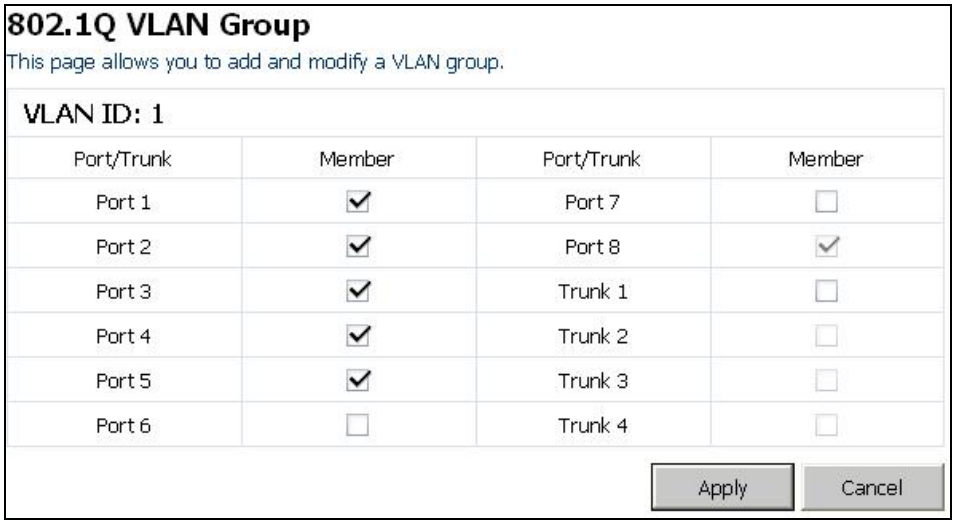
Rychlost pro tento port je nastaven na 1000 Mbit/s Full Duplex, aby byla zajištěna dostatečná rezerva pro provoz. Je zapnuta i kontrola přenosu.



Obr.36 Konfigurace portů

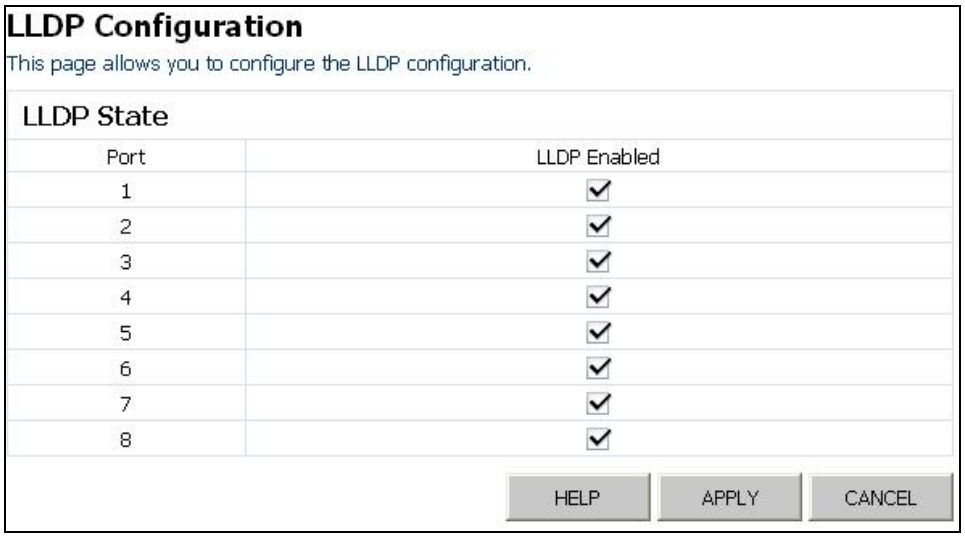
Pro zbylé porty na přepínači je nastavena rychlost na 100 Mbit/s, která plně stačí pro připojení pracovních stanic.

Pokud by v budoucnu některé ze stanic tato rychlost nestačila, je možné nastavit vyšší přenosovou rychlost.



Obr.37 Nastaveni portu do VLAN obchodní oddělení

Porty 1 až 5 jsou seskupeny do jedné VLAN které odpovídá ekonomickému oddělení. Porty 1 a 6 tvoří další VLAN.



Obr.38 Nastaveni LLDP

Jedná se o standard 802.1ab, který definuje vzájemné objevení přepínačů, směrovač ve stejném segmentu sítě, přičemž si tato zařízení vyměňují informace mezi sebou, a tak mohou pružně reagovat na provoz v síti.

Nastavení dalších přepínačů bude následovat pouze v textové podobě.

Přepínač 2.

IP adresa je nastavena na 172.16.0.3, maska 255.255.255.224 a Gateway 172.16.0.1. Porty 7 a 8 jsou nastaveny na parametr Trunk, který patří do protokolu Spanning Tree.

Pro tyto porty je nastavena rychlost přenosu 1000 Mbit/s FD. Porty 1 až 6 je nastavena na rychlost přenosu 100 Mbit/s FD. Vytvořena je VLAN pro Ekonomické oddělení, kde jsou zapojeny 4 pracovní stanice a printserver pro tiskárnu. Zapnuta je kontrola a řízení přenosu.

Přepínač 3.

IP adresa je nastavena na 172.16.0.4, maska 255.255.255.224 a Gateway 172.16.0.1. Port 8 je nastaven na parametr Trunk, který patří do protokolu Spanning Tree.

Pro tyto porty je nastavena rychlost přenosu 1000 Mbit/s FD. Porty 1 až 7 je nastavena rychlost přenosu 100 Mbit/s FD.

Vytvořeny jsou zde tří VLAN pro vedení, (3 pracovní stanice), vývoj (2 pracovní stanice) a prezenční místnost.

Přepínač 4.

IP adresa je nastavena na 172.16.0.66, maska 255.255.255.224 a Gateway 172.16.0.65. Porty 1 až 8 jsou nastaveny na rychlost přenosu 100 Mbit/s FD.

Vytvořeny jsou zde 4 VLAN - sklad, (2 stanice), expedice (2 stanice), technologie (2 stanice) a technici (1 stanice).

Přepínač 5.

IP adresa je nastavena na 172.16.0.58, maska 255.255.255.248 a Gateway 172.16.0.57.

Porty 1 až 8 jsou nastaveny na rychlost přenosu 1000 Mbit/s FD, protože tento přepínač je umístěn v serverovně, kde propojuje aplikačními servery s hlavním routerem.

Vytvořeny jsou dvě VLAN. Každý ze serverů má svoji vlastní VLAN z důvodu bezpečnosti.

5.11 Hlavní Server

Hlavní router je počítač, který umožňuje směrovat síťový provoz, spojuje jednotlivé segmenty sítě, překládá pakety z jedné sítě do druhé.

Server podle návrhu obsahuje celkem 6 rozhraní. Jednotlivá rozhraní jsou rozdělena následovně:

- eth0 - Počítačová síť v administrativní budově
- eth1 - Aplikační a ekonomický server
- eth2 - Páteřní bezdrátový směrový spoj(Routerboard)
- eth3 - Konektivitu do Internetu
- eth4 - Směrový bezdrátový spoj na vrátnici firmy
- eth5 - Přístupový bod umístěný v konferenční místnosti

Operační systém

Linuxová distribuce Slackware byla zvolena jako vhodná pro běh na hlavním serveru. Důvodem je nenáročná instalace, uživatelsky přívětivá administrace.

Routování mezi jednotlivými rozhraními zjistíme pomocí příkazu:

```
cat /proc/sys/net/ipv4/ip_forward
```

Příkaz vypsal 0, což znamená, že routování není zapnuto, proto tímto příkazem routování zapneme.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

DNS server

Kromě samotného routování poběží na serveru ještě DNS server BIND (Berkeley Internet Name Domain), což je kompletní implementace výše zmiňovaného DNS serveru. Přesto že se hodí spíše pro nasazení ve velkých sítích, nic nebrání použití ani v tomto konkrétním případě.

Z důvodů bezpečnosti je vhodné nastavit, aby BIND naslouchal požadavkům pouze na lokálních rozhraních. Důležitým

nastavením je taky nechat posílat dotazy jmenným serverům poskytovatele.

DHCP server

Další služba která poběží na serveru je DHCP server určený pro síťové rozhraní eth0.V linuxu je jako server použit program DHCPd.

```
# konfigurační soubor programu DHCPd
# Sample /etc/dhcpd.conf
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.224;
option broadcast-address 172.16.0.31;
option routers 172.16.0.1;
option domain-name-servers 172.16.0.1;
option domain-name "hps.cz";

subnet 172.16.0.0 netmask 255.255.255.224 {
   range 172.16.0.7 172.16.0.30; }
```

Firewall

Konektivita do internetu bude zajištěna pomocí veřejné IP adresy od poskytovatele, z tohoto důvodu bude potřeba použít při komunikaci do internetu překlad adres (NAT). Použití NAT je výhodné i z důvodu bezpečnosti, kdy se z Internetu nelze dostat na vnitřní síť. V tomto konkrétním případě, ale potřebujeme, aby fungoval mail server, který je až za NAT. Řešením je použití forward portu potřebných pro provoz mail serveru.

Na operačním systému Linuxu je firewall realizován pomocí iptables. V příloze je ukázka jednoduchého firewallu, který je realizován pomocí iptables, pro ochranu vnitřní sítě proti útokům z Internetu.

6 Závěr

Bezdrátové sítě jsou v dnešní době jedním z nejrychleji se rozvíjejícím odvětvím. Prostřednictvím bezdrátové technologie je možné provozovat počítačové sítě i z míst, kde to dříve bylo nemyslitelné. Oproti klasickým sítím nabízejí bezdrátové sítě výhody jako je mobilita, nižší náklady na budování a vyšší efektivnost.

Ve svém návrhu počítačové sítě jsem použil klasické „drátové„ prvky stejně tak jako bezdrátové. Snahou bylo dodržet požadavky, které měli majitelé firmy.

Firemní síť se nachází v několika budovách. Spojení mezi těmito budovami je v návrhu realizované pomocí bezdrátové technologie. Díky tomu bylo dosaženo úspor nákladů a nic nebrání do budoucna možným úpravám.

Samotný návrh obsahuje nákres topologie sítě, kde jsou zakresleny jednotlivé stanice, stejně tak jako použité aktivní síťové prvky s konkrétním nastavením.

Návrh byl majiteli přijat a v současné době je návrh realizován. Firemní síť by měla být v provozu od 1.července 2007, kdy začne provoz v nových prostorách firmy.

7 Zdroje

Wendell O.:*Počítačové sítě - Bez předchozích znalostí*, ComputerPress Brno 2005, ISBN 80-251-0538-5

Zandl,P.:*Bezdrátové sítě WiFi praktický průvodce*, ComputerPress Brno 2003, ISBN 80-7226-632-2

Pužmanová,R.:*Širokopásmový Internet - Přístupové a domácí sítě*, ComputerPress Brno 2003,ISBN 80-251-0139-8

Bigalow,S.J.:*Mistrovství v počítačových sítích*, ComputerPress Brno 2004, ISBN 80-251-0178-9

Dostálek,L. Kabelová,A.:*Velký průvodce protokoly TCP/IP a systém DNS*, ComputerPress Brno 2000, ISBN 80-7226-323-4

Janeček, J., Bílý, M.: *Lokální sítě*. Skripta ČVUT, Praha 1997

Bezdrátové lokální sítě WLAN podle IEEE [online]. Pužmanová,R.: [2007-04-18]. Dostupný z WWW: <http://www.lupa.cz/clanky/bezdratove-lokalni-site-wlan-podle-ieee-ii/>

IEEE 802.11[online]. Wikipedie [2007-04-19] Dostupný z WWW: <http://cs.wikipedia.org/wiki/IEEE_802.11>

802.11g: rychlejší WiFi? [online]. Pužmanová,R.: [2007-04-19] Dostupný z WWW: <http://www.lupa.cz/clanky/802-11g-rychlejsi-wifi/>

Tuning internetového připojení - DNS, SMTP [online]. Světlík,O: [2007-04-22] Dostupný z WWW: <http://www.root.cz/clanky/tuning-internetoveho-pripojeni-dns-smtp/>

Linux jako internetová gateway [online]. Vondráček,J: [2007-04-18] Dostupný z WWW: <http://www.root.cz/clanky/linux-jako-internetova-gateway/>

Linuxové DMZ [online]. Vymazal,M: [2007-04-13] Dostupný z WWW: <http://www.abclinuxu.cz/clanky/show/15988>

Reference Manual [online]. MikroTik OS: [2007-04-02] Dostupný z WWW: <http://www.mikrotik.com/testdocs/ros/2.9/>

DHCPd server [online]. Linux Dokumentation Projekt [2007-04-02] Dostupný z WWW: <http://tldp.org/HOWTO/DHCP/x369.html>

Iptables - stavový firewall [online]. Poloch,R: [2007-04-14] Dostupný z WWW: <http://www.owebu.cz/linux/vypis.php?clanek=880>

Zásady návrhu síťové infrastruktury [online]. Urbiš,M: [2007-04-9] Dostupný z WWW:<http://svetsiti.cz/view.asp?rubrika=Tutorialy& temaID= 231&clanekID=232>

Tutoriál o VLAN [online]. Luhový,K: [2007-04-12] Dostupný z WWW: <http://svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=237&clanekID =238>

Česká Wikipedia [online]. [2007-04-12] Dostupný z WWW: <http://cs.wikipedia.org>

Zdroje obrázků

(1) Zandl, P.:*Bezdrátové sítě WiFi praktický průvodce*, ComputerPress Brno 2003, str.7, ISBN 80-7226-632-2

(2) Zandl, P.:*Bezdrátové sítě WiFi praktický průvodce*, ComputerPress Brno 2003, str.8, ISBN 80-7226-632-2

(3) *Bezdrátové LAN sítě – WLAN* [online].Mallat,J.: [2007-05-01] Dostupné z WWW: <http://hps.mallat.cz/view.php?cisloclanku= 2003091101>

(4) *Bezdrátové LAN sítě WLAN* [online].Mallat J.: [2007-05-01] Dostupné z WWW: <http://hps.mallat.cz/view.php?cisloclanku= 2003091101>

(5) Zandl, P.:*Bezdrátové sítě WiFi praktický průvodce*, ComputerPress Brno 2003, str.128, ISBN 80-7226-632-2

(6) Zandl, P.:*Bezdrátové sítě WiFi praktický průvodce*, ComputerPress Brno 2003, str.131, ISBN 80-7226-632-2

(7) *InShop.net e-shop*:[online]. Dostupné z WWW: <http://www.i4shop.net/cz/iObchod/Cat.asp?ca=16&it=52>

(8) *Lan-Shop e-shop*:[online]. Dostupné z WWW:<http://www.lan-shop.cz/img/d-19224>

(9) *CzechComputers e-shop*:[online]. Dostupné z WWW: <http://www.czechcomputer.cz/product.jsp?artno=34039>

(10)*Levi e-shop*: :[online]. Dostupné z WWW: <http://www.bgslevi.cz/produkt_detail.php?id=40739>

Zdroje tabulek

(1) Zandl, P.:*Bezdrátové sítě WiFi praktický průvodce*, ComputerPress Brno 2003, str.17, ISBN 80-7226-632-2

(2) Zandl, P.:*Bezdrátové sítě WiFi praktický průvodce*, ComputerPress Brno 2003, str.17, ISBN 80-7226-632-2

(3) *Porovnání WLAN* [online]. Pužmanová,R.:[2007-03-18] Dostupné z WWW: <http://www.lupa.cz/clanky/802-11g-rychlejsi-wifi/>

(4) *Specifikace použitých zabezpečení* [online].Pužmanová,R.: [2007-03-17] Dostupné z WWW:<http://www.lupa.cz/clanky/wlan-konecne-bezpecne>

(5) *Odolnost proti útoku* [online].Pužmanová,R.:[2007-03-14] Dostupné z WWW:<http://www.lupa.cz/clanky/wlan-konecne-bezpecne/>

(6) Vhodnost nasazení [online].Pužmanová,R.: [2007-03-14] Dostupné z WWW:<http://www.lupa.cz/clanky/wlan-konecne-bezpecne/>

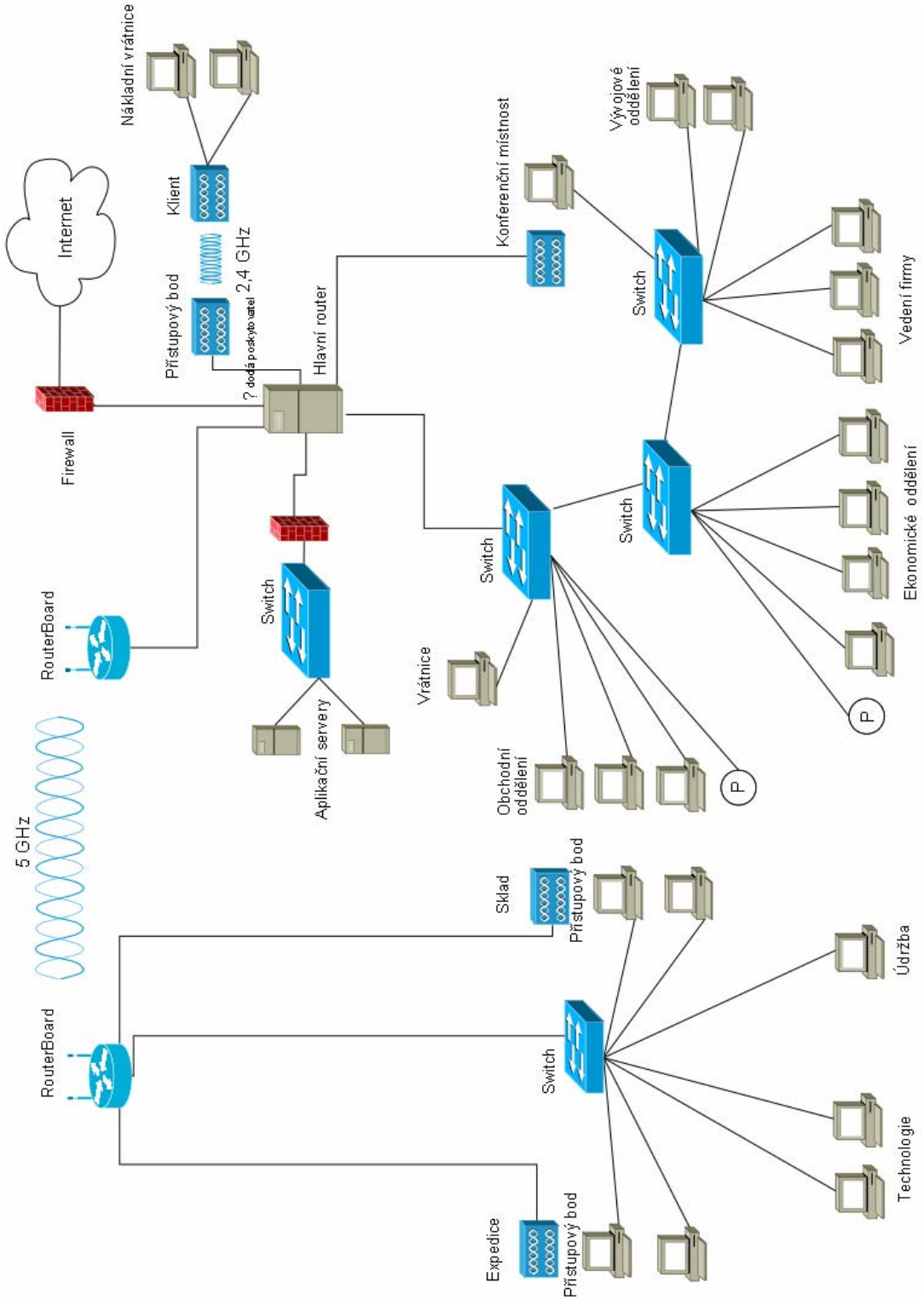
8 Seznam Příloh

Příloha A - Topologie navrhované sítě s popisem oddělení

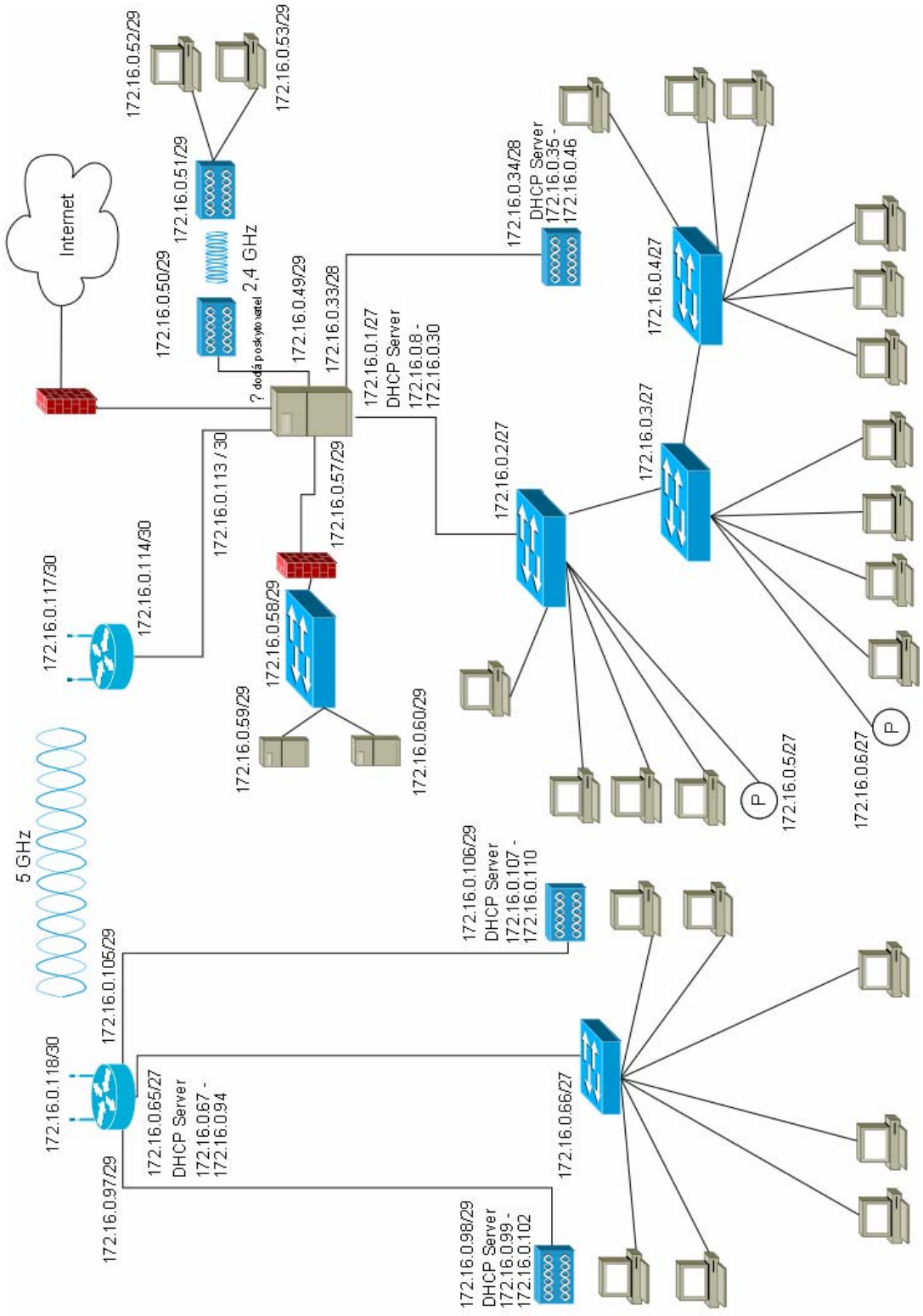
Příloha B - Topologie navrhované sítě s konkrétními IP adresami

Příloha C - Jednoduchý firewall pomocí iptables

Příloha A


Nákladní vrátnice
Klient
Internet
2,4 GHz
Přístupový bod
? dodá poskytovatel
Hlavní router
Konferenční místnost
Vývojové oddělení
Switch
Vedení firmy
Firewall
RouterBoard
Switch
Aplikační servery
Switch
Vrátnice
Obchodní oddělení
Switch
Ekonomické oddělení
P
P
5 GHz
RouterBoard
Sklad
Přístupový bod
Switch
Údržba
Technologie
Expedice
Přístupový bod

Příloha B


Internet
172.16.0.52/29
172.16.0.53/29
172.16.0.51/29
172.16.0.50/29
2.4 GHz
? dodá poskytovatel
172.16.0.49/29
172.16.0.33/28
172.16.0.34/28
DHCP Server
172.16.0.35 -
172.16.0.46
172.16.0.1/27
DHCP Server
172.16.0.8 -
172.16.0.30
172.16.0.113 / 30
172.16.0.57/29
172.16.0.117/30
172.16.0.114/30
172.16.0.58/29
172.16.0.59/29
172.16.0.60/29
172.16.0.2/27
172.16.0.3/27
172.16.0.4/27
172.16.0.5/27
172.16.0.6/27
5 GHz
172.16.0.105/29
172.16.0.118/30
172.16.0.65/27
DHCP Server
172.16.0.67 -
172.16.0.94
172.16.0.97/29
172.16.0.106/29
DHCP Server
172.16.0.107 -
172.16.0.110
172.16.0.66/27
172.16.0.98/29
DHCP Server
172.16.0.99 -
172.16.0.102

Příloha C

Jednoduchý firewall pomocí iptables

```
#všechny pakety budou zahozeny
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
#nastavení transparentní proxy
iptables -t nat -A PREROUTING -p tcp -i ! eth3 -d ! [ip dodá posky-
tovatel] --dport 80 -j REDIRECT --to-port 3128
#zprovoznění IP maškarády
iptables -t nat -A POSTROUTING -o eth3 -j SNAT --to [ip dodá posky-
tovatel]
#ochrana proti syn zahlcením
iptables -N syn-flood
iptables -A syn-flood -m limit --limit 1/s --limit-burst 4 -j RETURN
iptables -A syn-flood -j DROP
#optimalizace cest
iptables -t mangle -A PREROUTING -p tcp --sport ssh -j TOS --set-tos
Minimize-Delay
iptables -t mangle -A PREROUTING -p tcp --dport ssh -j TOS --set-tos
Minimize-Delay
#předávání z vnější do vnitřní sítě - jenom pro dříve navázaná spo-
jení
iptables -A FORWARD -i eth3 -o eth0 -m state --state
ESTABLISHED,RELATED -j ACCEPT
#logování zahozených paketů
iptables -A FORWARD -m limit --limit 12/h -j LOG --log-prefix "for-
ward drop: "
#přístup k jednotlivým službám
iptables -A INPUT -i eth3 -p TCP --dport 22 -j ACCEPT #SSH server
iptables -A INPUT -i eth3 -p TCP --dport 25 -j ACCEPT #SMTP server
iptables -A INPUT -i eth3 -p TCP --dport 53 -j ACCEPT #DNS server
TCP
iptables -A INPUT -i eth3 -p TCP --dport 80 -j ACCEPT #WWW server
iptables -A INPUT -i eth3 -p TCP --dport 110 -j ACCEPT #POP3 server
#propuštění pingu
iptables -A INPUT -i eth3 -p ICMP --icmp-type echo-request -j ACCEPT
#povolení localhostu
iptables -A INPUT -i lo -j ACCEPT
#ostatní packety zahodí přitom dochází logování
iptables -A OUTPUT -j LOG --log-prefix "OUTPUT drop: "
```

ÚDAJE PRO KNIHOVNICKOU DATABÁZI

Název práce	Návrh počítačové sítě s využitím WiFi technologie
Autor práce	Tomáš Křížek
Obor	Informační technologie
Rok obhajoby	2007
Vedoucí práce	Ing. Miloslav Macháček
Anotace	Návrh počítačové sítě s konkrétním popisem nastavení na jednotlivých síťových zařízeních
Klíčová slova	WiFi , bezdrátová síť, IEEE 802.11a, 802.11b, 802.11g, WPA