Jan Bicek
Mikrovlnné spoje a datové přenosy v pásmu 2,4 GHz

Pedagogická fakulta Jihočeské univerzity
Katedra fyziky

Mikrovlnné spoje a datové přenosy v pásmu 2,4 GHz

diplomová práce

Autor: Jan Bicek

Vedoucí diplomové práce: PaedDr. Petr Adámek, Ph.D.

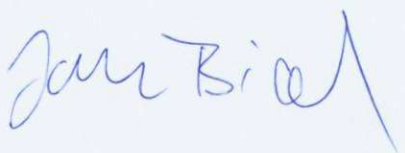
Knihovna JU - PF
3 1 1 5 1 7 1 7 0 1

České Budějovice 2005

Prohlášení:

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně, pouze s použitím literatury a zdrojů uvedených v části Seznam použité literatury.

V Českých Budějovicích 20.listopadu 2005



Obsah

1. Úvod

Bezdrátové sítě se stávají stále neodmyslitelnější součástí našeho života a jejich vliv na naše životy neustále roste. Typickým příkladem mohou být GSM sítě a mobilní telefony v nich zapojené, bez kterých si leckdo nedokáže již dnes představit svůj život. Ano, sítě pro mobilní telefony, to byl obrovský pokrok, dnes ale toto již začíná být málo. Na kapacitu bezdrátových sítí jsou s rostoucími požadavky na přenos multimédií kladeny stále vyšší nároky a sítě pro mobilní telefony se začínají prolínat s datovými bezdrátovými sítěmi pracující na protokolech TCP/IP (Transmition Control Protocol / Internet Protocol).

Cílem práce je vytvořit text vhodný např. pro IT koordinátora školy, ve kterém bude popsána část z celkového spektra o bezdrátových sítí ve 2,4 GHz a sice část o WiFi sítích a ukázat teoreticky i prakticky realizaci počítačové sítě založené na této technologii a to od návrhu spoje až po konfiguraci WiFi zařízení, který čtenáři pomůže se v problematice zorientovat, jelikož česky psané literatury o tomto tématu je velice málo. Rád bych také poukázal na některé možností využití podporovaných WiFi karet a následné síťové operace v operačním systému GNU Linux, jelikož tato kombinace nabízí opravdu velké možnosti a ve školním prostředí, kde peněz, na rozdíl od starších dnes již dosluhujících počítačů, není nazbyt, dokáže téměř zázraky.

Tuto práci jsem se rozhodl vytvořit proto, že se o danou problematiku již několik let živě zajímám a rád bych využil i znalostí, zkušeností a dovedností získaných v zaměstnání, kde se již přes rok věnuji právě bezdrátovým počítačovým sítím.

2. Obecný popis mikrovlnných spojů

Na začátek bych rád uvedl něco z historie Wifi, význam různých zkratek používaných dále v práci, vývoj standardů sdružení IEEE (The Institute of Electrical and Electronics Engineers) týkajících se právě bezdrátových přenosů, vlastnosti bezdrátových komponent – od konektorů až po samotná zařízení pro příjem a vysílání vf signálu, antén atd.

2.2 Historie

Bezdrátové sítě existují od roku 1992, tehdejší zařízení ale pracovala na provozních rychlostech hluboko pod 1 Mbit/s. V té době také chyběl jakýkoliv standard, takže bylo nutné používat síťové prvky stejného výrobce - výrobky různých výrobců vzájemně nebyli kompatibilní a nebylo možné je propojovat mezi sebou. Tato situace se významně zlepšila po roce 1997 kdy byl přijat standard IEEE 802.11 - o přenosu infračerveného signálu a o přenosu signálu v tzv. bezlicenčním nekoordinovaném ISM (Industrial Scientific Medical) pásmu na frekvencích 2,4 GHz ÷ 2,4835 GHz, tedy zjednodušeně řečeno v pásmu 2,4 GHz a rychlosti od 1 Mbit/s do 2 Mbit/s (infračervený signál zůstal součástí standardu, ale prakticky není implementován) , jímž jsou moderní WLAN (Wireless LAN – bezdrátové sítě) sítě definovány a standardizovány. IEEE 802.11 dále definoval způsob přenosu signálu po fyzickém médiu, což jsou v zde radiové vlny, a způsob řešení kolizí protokolem CSMA/CA (Carrier Sense Multiple Access With Collision Avoidance), který pracuje na principu předcházení kolizím s pozitivním potvrzováním.

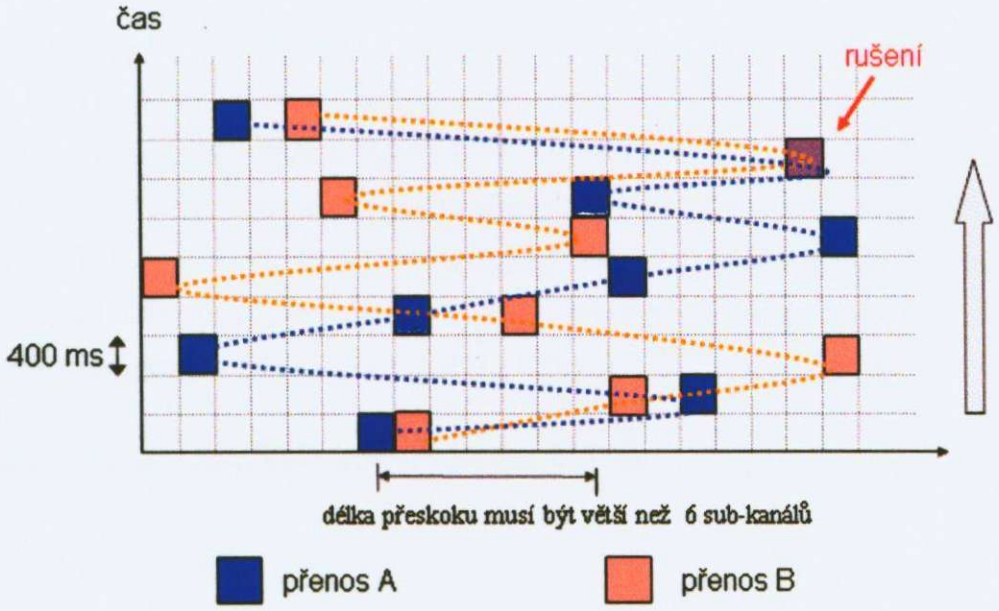
Dále standard 802.11 nikterak neomezoval používanou technologii přenosu po fyzické vrstvě. Dle nařízení FCC (Federal Communications Commission - Federální komunikační komise Spojených států amerických) a ETSI (European Telecommunications Standards Institute – Evropský ústav pro telekomunikační normy) se ale v ISM pásmu smí vysílat pouze pomocí rozprostřeného spektra, tzn. FHSS (Frequency hopping spread spectrum), DSSS (Direct sequence spread spectrum), OFDM (Orthogonal frequency division multiplex, tady ale pozor, nepracuje s rozprostřeným spektrem. Viz dále v kapitole

o IEEE 802.11g.) a PBCC (Packet binary convolutional coding) což je proprietární řešení firmy Texas Instrument umožnující ještě větších rychlostí. Něco blíže jednotlivým systémům FHSS a DSSS. [1, 2, 3]

2.2.1 - Popis technologií FHSS a DSSS

FHSS (Frequency hopping spread spectrum) – Frekvenční poskoky

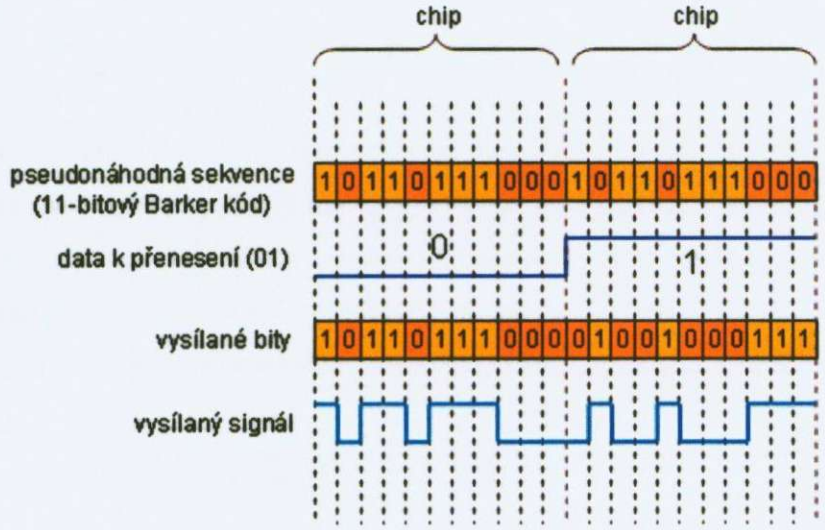
Technologie frekvenčních poskoků má svůj původ ve vojenské technice. Je poměrně těžko odposlouchávatelná a do pásma o šířce 83,5 MHz se vejde teoreticky 26, prakticky však okolo 15 přístupových bodů, což je oproti dalším technologiím pracujícím s rozprostřeným spektrem poměrně hodně. Tato technologie pracuje tak, že si rozdělí pásmo na 79 kanálů o šířce 1 MHz a radiový signál pak pseudonáhodně přeskakuje z jednoho kanálu na další. Na každém kanálu vysílá maximálně 400 ms a za 30 sekund vystřídá alespoň 75 kanálů. [2]



Obr. 1: Schéma přeskoků u DFSS

DSSS (Direct sequence spread spectrum) – Přímá sekvence

Zařízení pracující na tomto základu rozprostřou na 22 MHz širokém kanálu za pomocí matematického kódování (XOR) vysílanou zprávu. Přijímač dekóduje zprávu opačným postupem ke kódování. Jak si lze jednoduše spočítat, dají se takto do daného pásma ISM vtěsnat pouze 3 celé kanály, aniž by se rušily. [2]



Obr. 2: Příklad matematického skládání signálu (XOR)

Ačkoli to byl pokrok, stále bylo nejméně 5 různých komerčních produktů držících se 802.11 standardu firem jako Alvarion (PRO.11 a BreezeAccess-II), Netwave Technologies (AirSurfer Plus a AirSurfer Pro), Symbol Technologies (Spectrum24) a Proxim (OpenAir) což stále nebylo zcela vhodné (a někdy ani žádané) pro propojování sítí pomocí různých technologií dle 802.1 standardu. Slabostí specifikace bylo právě její příliš obecné zadání, které je spíše doporučením než konkrétní specifikací a tak byla zhruba ve dvou letech doplněna a vznikl standard IEEE 802.11b.

2.2.2 - IEEE 802.11b a WiFi je na světě

2.2.2.1 - IEEE 802.11b

Novému standardu bylo do vínku přidáno několik důležitých vlastností. Jednou a možná nejdůležitější vlastností byla rychlost. Jak je výše popsáno, standard 802.11 byl tvořen pro rychlosti do 2 Mbit/s což již moderním podmínkám přestalo dostačovat a tak standardizační výbor IEEE zvolil 11 Mbit/s jako maximální datový tok, který muselo zařízení vyhovující standardu dokázat za ideálních podmínek přenést. Tímto rozhodnutím se technologie FHSS (Frequency hopping spread spectrum), která se v 802.11 používala téměř stejně často jako technologie DSSS (Direct sequence spread spectrum), nedostala do 802.11b specifikace, protože, nedokázala přenést po fyzickém médiu více než 2 Mbit/s bez

překročení limitů FCC a ETSI. Modulace DSSS byla tedy jedinou možnou volbou.

Ačkoli nový standard byl již konkrétnější, stále nevylučoval různé interpretace a právě proto vznikla v roce 1997 organizace WECA (Wireless Ethernet Compatibility Aliance), která si dala za cíl ověřovat kompatibilitu konkrétních produktů s tímto (a dalšími, viz dále) standardy a, což je zřejmě ještě mnohem podstatnější, jejich vzájemnou interoperabilitu. Organizaci založily významné firmy vyrábějící ethernetová bezdrátová zařízení jako mezinárodní nevýdělečnou asociaci, která po ověření výrobku v nezávislé laboratoři dle předem veřejně známých podmínek udělila či neudělila logo o certifikaci.

Obr 3: Logo sdružení WECA

Ještě něco málo o této organizaci, které vděčíme za takový rozmach bezdrátového internetu. Se stále větší oblibou zkratky WiFi a v reakci na různé obtíže, které panovaly se zkratkou WECA se nechala organizace přejmenovat na poněkud pochopitelnější WiFi aliance (http://www.wi-fi.org)a zaregistrovala si ochranou známku WiFi (obrázky 4, 5, 6, 7). [4]

Obr. 4: Jedno z log certifikovaných výrobků pro WiFi a splňující IEE 802.11a,b,g

Obr. 5: Logo WiFi Aliance

Obr. 6: jedno z log certifikovaných výrobků pro WiFi a splňující IEE 802.11a,b,g

Obr. 7: Jedno z log certifikovaných výrobků pro WiFi a splňující IEE 802.11a,b,g

2.2.2.2.- IEEE 802.11g

Poslední standard který se v poslední době (léto až podzim 2005) u nás v České republice začíná rozšiřovat je IEEE 802.11g. Lze říci, že tento standard zažívá „boom", výrobci vyrábějí bezdrátové komponenty a tyto pak montují do obrovské skupiny zařízení a to i do zařízení ve kterých bychom je dříve ani nečekali. Samozřejmostí jsou notebooky s vestavěným WiFi adaptérem, PDA(Personal Digital Assistant), WiFi – USB zařízení o velikosti běžné USB klíčenky, ale také bezdrátové kamery, DVD přehrávače, multimediální digitální ukládací zařízení a dále. Na produktovém školení firmy D-Link® firma prezentovala svoji vizi digitální domácnosti, kde bylo veškeré multimediální a zabezpečovací zařízení domácnosti propojeno pomocí bezdrátové sítě, za účelem maximalizování pohodlí příbytku.

Problém s IEEE 802.11 byl u nás (v Evropě) ten, že používá modulaci ODFM, která ovšem nepracuje s pomocí rozprostřeného spektra a tudíž nesměla být používána v ISM pásmu (ještě větší problémy s prosazením měl standard IEEE 802.11a pracující v pásmu 5GHz, kde se střetl „americký" a „evropský" pohled na danou problematiku) jak ETSI, u nás ČTÚ (Český Telekomunikační Úřad) vyžadovali. Naštěstí ale bylo ISM pásmo i u nás uvolněno k používání pro ODFM a díky tomu můžeme používat i WiFi výrobky

pracující na základě normy IEEE 802.11g a z toho vyplývající rychlost 54 Mbit/s. Dle standardu IEEE 802.11g spolu musí být schopny současně komunikovat zařízení dle normy IEEE 802.11b i IEEE 802.11g, čili na přístupový bod se musí být možné se připojit jak pomalejší IEEE 802.11b , tak rychlejší IEEE 802.11g technologií. Bohužel ale v situacích kdy to tak opravdu má fungovat a přístupový bod pracuje s oběma druhy klientů, tím pádem i s dvěma druhy modulací, není využit efektivně, režie přenosu neúměrně stoupá a přenosová rychlost se značně snižuje. [9]

2.2.3 – Přehled činnosti standardizační skupiny IEEE 802.11

Nyní si můžeme zrekapitulovat všechna ta písmenka za jedenáctkou:

802.11a - WLAN v pásmu 5 GHz a s rychlostí až 54 Mbit/s, standard zveřejněn v roce 1999, v Evropě nepovolen pro venkovní vysílání, povolen pouze v zástavbě a s anténou dodanou výrobcem zařízení.

802.11b - WLAN v pásmu 2,4 GHz a s rychlostí až 11 Mbit/s. Viz výše.

802.11b-cor - úpravy MIB v 802.11b (MIB = management information base).

802.11c - definice procedur pro síťové mosty, bridge. Ve skutečnosti to s WLAN má jen málo společného, jde ale o užitečný standard pro přístupové body.

802.11d - Mezinárodní harmonizace. Se vznikem standardu 802.11 se ukázalo, že je potřeba mezinárodní kooperace a harmonizace. Zejména pásmo 5 GHz se používá v mnoha státech různě a bylo třeba tomu standardizaci přizpůsobit tak, aby nevycházela vstříc pouze potřebám USA a Japonska. Funguje tak, že *access point* vysílá *broadcast* pakety (pakety určené všem zařízením sítě) s kódem země (dle ISO 3166-1).

802.11e - rozšíření MAC (Medium Access Control) pro QoS. Zkratka QoS označuje službu Quality of Service zajišťující stavitelnou kvalitu služeb, důležitou například pro přenos multimédií či provozování IP telefonie na internetových linkách. Zjednodušeně řečeno je potřeba, aby datový tok s vyšší prioritou, což je například zmiňované internetové telefonování nebo *ssh* (secure shell), měl přednost před protokoly, které na interakci tolik

závislé nejsou. Příkladem protokolu nezávislého na rychlé interakci je např. internetová pošta, email, http (hyper text transport protokol) a další, kde chvilkový výpadek či delší odezva při výměně paketů nehrají roli. QoS se využívá nejen jak již bylo řečeno při přenosu různých multimédiích a v IP telefonii, ale i v aplikacích kriticky důležitých (aplikace jejichž selhání může mít za následek smrt osob, poškození životního prostředí apod.).

802.11f - Inter Access Point Protocol (IAPP) - Stávající specifikace 802.11 nezahrnují standardizaci komunikace mezi jednotlivými přístupovými body pro zajištění bezproblémového roamingu, tedy přechodu uživatele od jednoho přístupového bodu k druhému. V současné době tak produkty různých výrobců nejsou schopny spolu o roamingu bezproblémově komunikovat a při výstavbě větších sítí, kde se roaming předpokládá, je nutno používat přístupové body jednoho výrobce s jejich proprietárním řešením, nebo celou záležitost řešit mimo přístupové body. Je zde kladen značný důraz na bezpečnost.

802.11g - zvýšení rychlosti v pásmu 2,4 GHz na 20 Mbit/s se zpětnou kompatibilitou k 8021.b, viz výše.

802.11h - změny v řízení přístupu k spektru 5 GHz, které by měly reflektovat připomínky regulátorů evropských zemí tak, aby bylo možno sítě v pásmu 5 GHz využívat i mimo budovy. Jak již jsem naznačil dříve, podmínky pro vysílání v pásmu 5 GHz jsou mnohem náročnější než v USA či Japonsku, zejména kvůli Evropou připravované síti HIPERLAN/2 (Evropská obdoba bezdrátových sítí 802.11a, ale vývojově dále. Její zařízení musí podporovat dynamickou volbu kmitočtu DFS - Dynamic Frequency Selection a automatickou regulaci výkonu TPC - Transmission Power Control).

802.11i - zlepšení bezpečnosti v 802.11 bezdrátových sítích vylepšením autentizačního a šifrovacího algoritmu. Velmi důležité a schváleno v červnu 2004. Šifrování WPA2.

802.11j – rozšíření pro Japonsko (jiné frekvenční rozsahy).

802.11k - tento projekt má definovat měření a správu radiových zdrojů tak, aby vyhovovaly novým vysokofrekvenčním radiovým sítím a zajistili co největší přenosové

rychlosti.

802.11l – rezervováno.

802.11m – toto rozšíření se zabývá hlavně zdokonalením dokumentace standardů jako takových. Někdy je nazýván „cleaner 802.11".

802.11n – zvýšení propustnosti.

802.11o – rezervováno.

802.11p – též nazýván bezdrátový přístup do prostředí motorových vozidel , definuje vylepšení 802.11 požadované pro aplikace inteligentního transportního systému (ITS), zahrnující datovou výměnu mezi rychle jedoucími vozidly a mezi těmito vozidly a stacionární infrastrukturou (v pásmu 5,9 GHz).

802.11q – rezervováno.

802.11r – hlavní použití tohoto plánovaného standardu je ve VoIP (Voice over Internet Protokol – telefonování internetem), pomocí mobilních telefonů navržených k práci na bezdrátové WiFi síti místo (nebo v součinnosti s) nyní používaných celulárních (buňkových) sítích.

802.11s – účelem tohoto zatím neschváleného standardu bude poskytnout protokol na automatické řízení tras mezi přístupovými body a zvolení nejkratší cesty pro pakety samoorganizující se WiFi sítě.

802.11T – účelem tohoto projektu je poskytnout množinu měřících metod a testovacích doporučení, které umožní výrobcům, nezávislým laboratořím, poskytovatelům i koncovým uživatelům měřit výkonnost zařízení a sítí standardu IEEE 802.11.

802.11u – tento standard má zajistit propojení s externími sítěmi „ne-IEEE 802.11" standardu (např. celulárními sítěmi mobilních telefonů).

802.11v – další přiblížení k mobilní komunikaci

802.11w – další posílení bezpečnosti.

[6, 7]

Jak vidno, v praxi si vystačíme s rozšířením "b" pro WiFi, s rozšířením "a" pro WiFi v pásmu 5GHz a s rozšířením "g" pro zvýšení rychlosti WiFi. Ostatní rozšíření označují funkce potřebné hlavně pro firemní a složitější sítě, či pro sítě dalších generací.

Nyní je třeba si přiblížit ISM frekvenční pásmo. V tomto nelicencovaném pásmu pracuje mnoho různých bezdrátových zařízení, například bluetooth produkty, v zahraničí domácí bezdrátové telefony, ale i mikrovlnné trouby (využívá se toho efektu, že tyto frekvence jsou pohlcovány molekulami vody při čemž jim dodají energii, která se na konec projeví např. ohřátou pizzou – v mikrovlnné troubě, ale také se projeví značnými problémy pro přenos signálu za deště ale hlavně skrz mokré překážky, jak se podrobněji zmíním později v kapitole 2.3). Kromě tohoto pásma se pro WiFi sítě vyhrazuje ještě pásmo 5 GHz, též ISM, které používá zatím technologie 802.11a, jenže jak už jsme si řekli, v Evropě není vítána a tak se čeká na jejího nástupce označovaného jako 802.11h, který již evropským předpisům vyhovuje. [3]

Frekvenční rozsah pásma ISM se ovšem liší země od země - v některých státech není povolené plné frekvenční spektrum, protože jeho části jsou již využívány pro jiné účely. Pro nás je příjemné, že ČTÚ povoluje použít plné frekvenční spektrum ISM (samozřejmě pokud se dodrží pravidla stanovená pro vysílání), jako je tomu v USA nebo ve většině Evropy, takže i výrobky koupené v USA se dají vcelku bez obtíží v ČR používat.

Region	Frekvenční rozsah v GHz	Počet kanálů
USA	2,4000 - 2,4835	79
Evropa (bez Fr. A Šp.)	2,4000 - 2,4835	79
Francie	2,4465 - 2,4835	27
Španělsko	2,445 - 2,475	35
Japonsko	2,471 - 2,497	23

Tabulka 1, povolené radiové frekvence pro WiFi sítě v pásmu 2,4 GHz. [1]

3. Realizace bezdrátového spoje

Jestliže chceme navrhnout a realizovat bezdrátové spojení, je třeba důkladného plánování, měření, plánování realizace a na konec samotná realizace. První plánování je víceméně teoretické a sice se rozhoduje, zdali má vůbec cenu použít bezdrátového spoje, jestli je to možné.

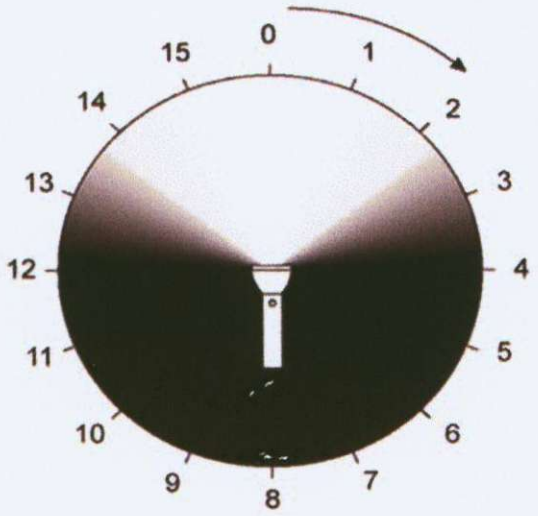
Prvním předpokladem pro kvalitní WiFi spoj je přímá viditelnost. Stanice musí „vidět" na přístupový bod. V cestě nesmí stát žádná překážka. Stromy, vedení vysokého napětí, zástavba, nebo jiný WiFi spoj je možný zdroj problémů, který se musí do návrhu připočítat a brát velmi vážně. Právě se stromy je značný problém hlavně v tom, že v průběhu roku a let, stromy opadávají, rozrůstají se a moknou. Mokrý strom v cestě zaručeně zničí jindy bezproblémový signál. Voda má totiž tu vlastnost že pohlcuje mikrovlnné záření. Neodráží jej jako jiné materiály, ale spotřebuje vysílanou energii na svůj ohřev. Této vlastnosti vody se využívá v mikrovlnných troubách, kde jsou téměř shodné frekvence jako frekvence 2,4 GHz ISM pásma, využívány k ohřevu potravin. Není třeba se ale obávat např. globálního oteplování. Vysílaná energie je zanedbatelná, navíc se se vzdáleností dále zmenšuje, takže její vliv je nepatrný. Dále bych rád vyvrátil některé fámy spojené se signálem WiFi a počasím. Velká část neznalých si myslí, že při hustém dešti či sněhové vánici se kvalita signálu zhoršuje až k nepoužitelnosti spoje, což ale není pravda, jak se můžeme přesvědčit v přiložených grafech v příloze 1. To co může zhoršovat signál, obzvláště u antén typu Yagi je, například sníh ležící na anténě. Pak je útlum signálu znát, ale padající sníh či průtrž mračen, jak již jsem psal, nevadí. [3]

Zde ještě jedna malá poznámka. Ano, pro kvalitní bezdrátový spoj ve WiFi pásmu je samozřejmě potřebná přímá viditelnost, na druhou stranu někdy není potřeba vysloveně kvalitní spoj a již v návrhu spoje se počítá s jistými nedostatky a proto je možno se pokusit i o spoj bez přímé viditelnosti, tento však musí být velice pečlivě proměřen, nesmí být na velkou vzdálenost, maximální vzdálenost klienta od přístupového bodu nesmí přesáhnout (20 ÷ 30) metrů a je opravdu třeba počítat s jistými nestálostmi a neduhy spoje.

Pro naplánování spoje je třeba vědět něco o anténách, signálu a vlastnostech šíření frekvencí ve WiFi pásmu vzduchem. Začněme anténami.

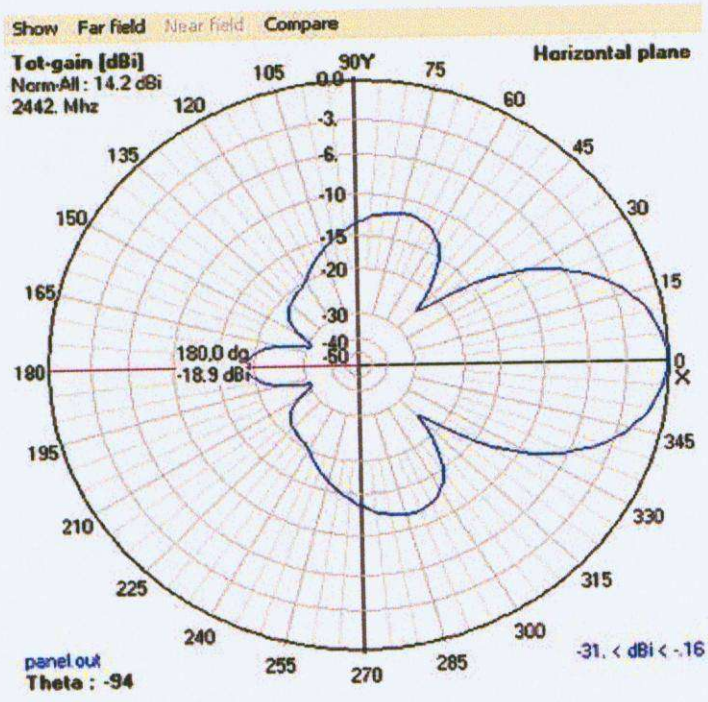
3.1 - Antény

Antén je velké množství druhů. Rozdělující se dle velikosti zisku antény, provedení, dle úhlu vyzařování, druhu antény, způsobu uchycení atd. Nejspíš nejdůležitější vlastností antény je její zisk. Zisk antény je vždy vyjádřen ve vztahu k referenční (srovnávací) anténě. Nejčastěji používanou referencí je izotropický zářič (takový zisk je označován dBi, další jednotkou je dBd, tedy decibel na dipól, tato jednotka je o 2,16 dB menší a zřejmě z obchodního hlediska výrobci raději užívají „větší" dBi). Ten ve skutečnosti neexistuje, jde o matematickou "fikci", představovanou vyzařujícím hmotným bodem. Jeho vyzařovacím diagramem je koule, výkon je tedy vyzařován rovnoměrně do všech částí prostoru stejně. Protože lze ale těžko srovnávat reálné antény s fiktivním zářičem, používá se často jako referenční anténa půlvlnný dipól. Dipól je anténa tvaru T o velikosti zářiče právě poloviny vlnové délky pásma, na kterém dipól pracuje. Dipólem se v praxi nahrazuje teoreticky definovaná izotropní anténa, která vyzařuje do všech stran beze ztrát. jehož zisk oproti izotropickému zářiči lze stanovit na 2,14 dB. Vyzařovací diagram reálné antény je vždy jiný, taková anténa tedy vyzařuje do některé části prostoru větší výkon, než by vyzářil tento hypotetický izotropický zářič. Dobrou pomůckou pro názornou ilustraci vyzařovacího diagramu antény je světlo kapesní svítilny, které je jejím reflektorem soustřeďováno do určité části prostoru, zatímco jinam svítilna nesvítí. Viz obrázek 8.



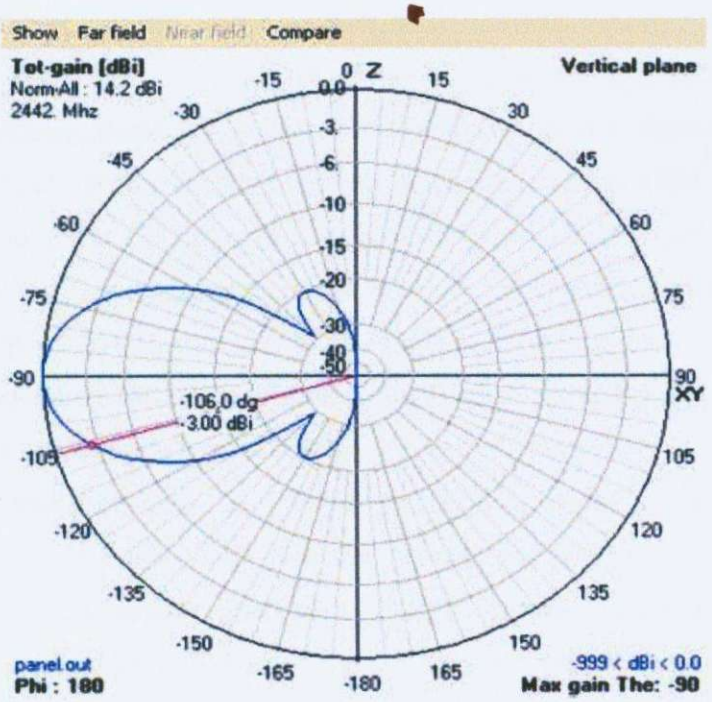
Obr. 8: Pro představ zisku a směrovosti antény.

Obrázky zisku, směrovosti a předozadních a předobočních poměrů u oblíbené tzv. panelové antény, tvořené čtyřmi soufázově napájenými dipóly před reflektorovou stěnou.

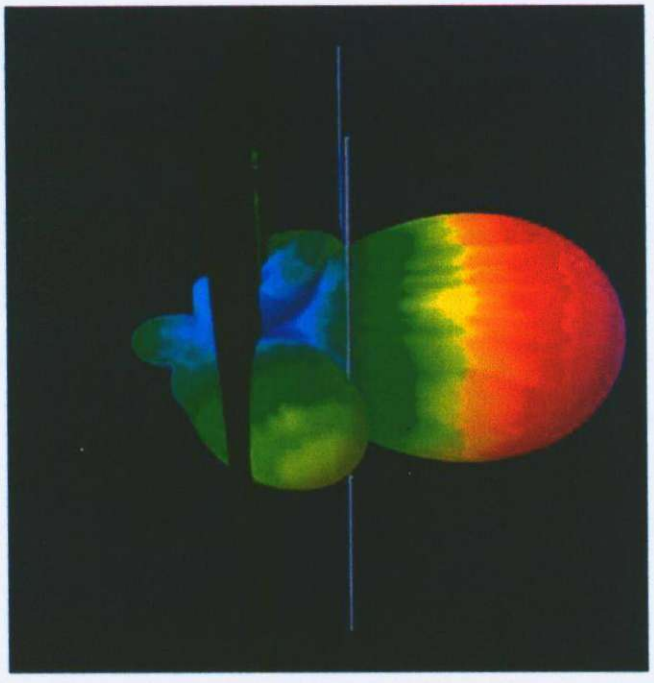


Obr. 9: Vyzařovací diagram panelové antény v horizontální rovině. Naznačen je zisk antény 14,2 dBi a předozadní poměr 18,9 dB.

JIHOČESKÁ UNIVERZITA
V ČESKÝCH BUDĚJOVICÍCH
PEDAGOGICKÁ FAKULTA
ÚSTŘEDNÍ KNIHOVNA -8-
Husova 458, 370 05 České Budějovice



Obr. 10: Vyzařovací diagram panelové antény ve vertikální rovině. Naznačen je opět zisk antény 14,2 dBi a úhel pro pokles -3 dB (16o).



Obr. 11: Trojrozměrná prezentace vyzařovacího diagramu panelové antény. Názorně ukazuje všechny popisované parametry

Tak vysokého zisku, jaký představuje reflektor kapesní svítilny, je možné prakticky dosáhnout jen u antény pracující v pásmu centimetrových vln, kde můžeme použít např. parabolického reflektoru. Rozměry antén totiž vždy vyjadřujeme v násobcích vlnové délky, na nižších kmitočtech proto rozměry antény vycházejí velké. ISM pásmo 2,4 GHz představuje vlnovou délku 12,3 cm. Půlvlnný dipól tedy bude 6,15 cm dlouhý, reflektor parabolické antény s opravdu slušným ziskem by mohl mít průměr 10 vlnových délek, tedy 1,2 metry. To je ještě přijatelné, ale zkuste si spočítat, jak by to dopadlo v případě antény pro FM rozhlas, laděné na 100 MHz (vlnová délka 3 m). Centimetrová a ještě kratší pásma jsou tedy doménou antén s vysokým ziskem.

Již tedy víme, že zisk je vlastně schopnost antény soustředit energii do požadovaného směru. U antén vždy platí tzv. princip reciprocity, anténa se tedy chová stejně, ať je použita pro příjem nebo pro vysílání. Anténa s úzkým svazkem umožní potlačit nežádoucí rušící signály a zároveň vysílat jen tam kam potřebujeme.

Dalším parametrem antény může být na příklad její vyzařovací úhel. Dle vyzařovacího úhlu dělíme antény na tři kategorie.

- Všesměrové - vysílají signál "všude kolem sebe" - tj. pokryjí úhel 360°. Když použiji příklad se světlem, bude takovou „anténou“ třeba svíčka.
- Sektorové - vyrábějí se v různých variantách, kdy pokryjí určitý sektor prostředí - např. 45°, 90°, ...
- Směrové - používají se na nejdelší spoje, vyzařují paprsek jedním směrem v úzkém pruhu, 3° ÷ 5°. V USA se povoleno směrovými anténami vysílat i vyšším výkonem, protože paprsek je opravdu úzký a nezarušuje prostředí. Snad proto je i nejdelší linka realizovaná běžně dostupnými komponenty právě v USA v Kalifornii a má 115km. Vysílací i přijímací výkon je 0,25 wattů. [3]

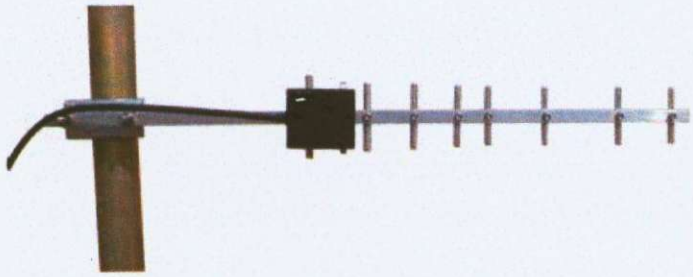
Dále jsou antény ještě děleny dle polarizace na lineární a na antény s kruhovou polarizací .Antény s kruhovou polarizací se dále dělí na pravotočivé a levotočivé a antény s lineární polarizací e dělí podle vysílací vysílací roviny na horizontální a vertikální. V praxi se používají hlavně antény lineární. Vhodnou volbou polarizace antény je možné se spojit i na silně zarušených místech, kde se dá volbou polarizace výrazně potlačit rušení od

okolních sítí.

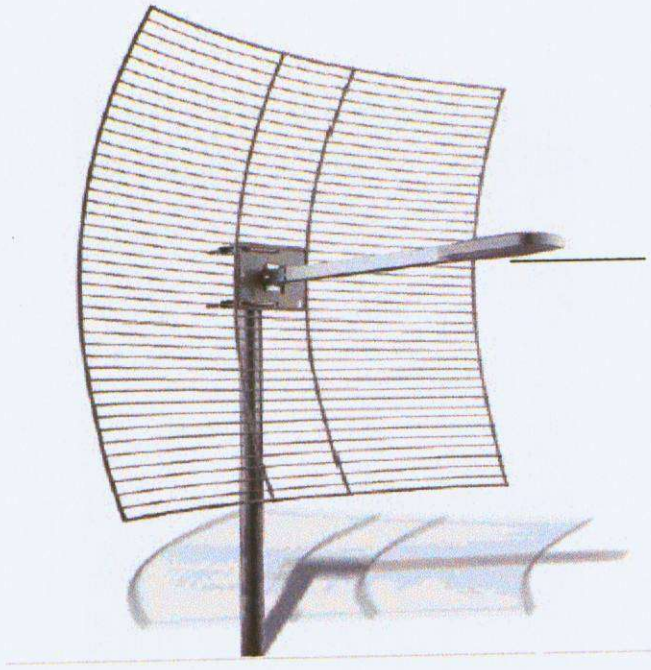
Aby bylo na spoji dosaženo maximálního možného výkonu, je nutné používat antény se stejnou polarizací. V případě že tomu tak není, je nutné počítat se ztrátami. Např. při příjmu lineárně polarizované signálu anténou šroubovicovou (která je určena pro příjem kruhově polarizovaného signálu) bude výsledný zisk o 3 dB menší. Horší situace nastávají při nesouhlasu směru kruhové polarizace, nebo otočení roviny lineární polarizace. V praxi pak může dojít k potlačení zisku o 16 až 24 dB, což vede prakticky k přerušení spojení.[3, 8]

Několik obrázků antén:

směrové antény:



Obr. 12: Anténa Yagi



Obr. 13: Směrová anténa 24 dbi – síto

Sektorová anténa:

Obr. 14: Sektorová anténa UNI – 7,5 dBi

všesměrové antény:

Obr. 15: Všesměrové antény v pouzdrech

Na závěr je třeba ještě vědět jakým typem konektoru je anténa připojována. Více ale v kapitole o konektorech.

3.2 - Kabely

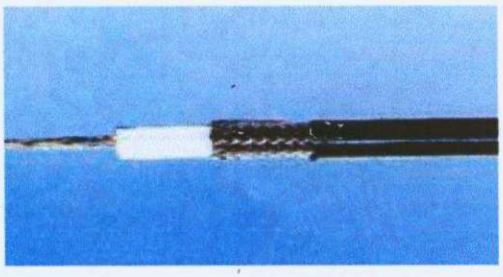
Dalším důležitým prvkem je kabeláž, a sice svod od zařízení pro bezdrátový WiFi přenos a antény. Tyto kabely jsou speciální vysokofrekvenční kabely a podle toho se s nimi musí i jednat. Na takovémto kabelu se již každý ohyb, každé neopatrné zacházení může projevit značným zvýšením útlumu a je nutné opravdu se ke kabelu správně „chovat". Výrobce u kabelu udává nejen útlum na metr, kdy jednotkou je dB/m, ale také například maximální poloměr ohybu, který je u kabelu dovolen, jeho rozměry, druh opletení apod.

Kabel se skládá z vodivého měděného jádra, nevodivého dielektrika, a to buď plného, nebo se vzduchovými mezerami, ze stínění, buď elektricky vodivá folie nebo síť z měděného drátu nebo měděná trubička a nakonec z opláštění. Z kvality provedení kabelu se odvíjí jeho parametry pro přenos, typicky útlum, ale také jeho cena. Více v přiložené tabulce různých druhů kabelů (tabulka 2) a podrobný přehled parametrů v tabulce 3 ke

kabelu Belden H1000 0,22 dB do 3 GHz. [3, 8]

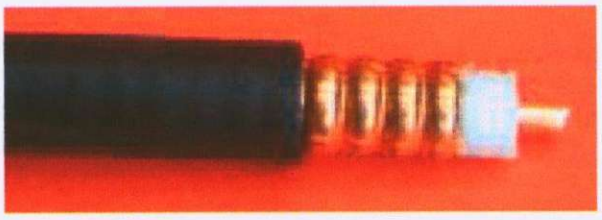
Kabel	útlum (dB/m)	orientační cena (Kč/m)
H125	0,35	15
H155	0,5	25
H1000	0,22	38
RLA10	0,22	50
RG58	0,79	11
RG213/214	0,37	30
LMR400	0,21	155
LMR195	0,62	75

Tabulka 2, útlum kabelů a jejich orientační cena.



Obr. 16: Levné kabely s jednoduchým stíněním

Obr. 17: Kvalitnější kabely používají fólii kombinovanou s opletením, zde RLF 10



Obr. 18: Nejjakostnější kabely mívají stínění tvořené měděnou trubkou a často teflonové nebo vzdušné dielektrikum.

Impedance ohm 50	Dielektrikum Fyz.pěna
Tolerance impedance ohm +/- 2,0	Průměr přes dielektrikum mm 7,15
Kapacita pF/m 80	Tolerance mm +/- 0,15
činitel zkrácení 0,83	Vnější vodič - fólie Cu
Max. ss odpor ve smyčce ohm/km 11	Vnější vodič - opletení Cu
Útlum při 10MHz dB/100m 1,2	Pokrytí opletením - % % 50
Útlum při 50MHz dB/100m 2,7	Průměr přes vnější vodič mm 7,8
Útlum při 100MHz dB/100m 3,9	Plášť PVC/PE
Útlum při 230MHz dB/100m 6,1	Průměr přes plášť mm 10,3
Útlum při 300MHz dB/100m 7	Tolerance mm +/- 0,20
Útlum při 470MHz dB/100m 7,3	Min. poloměr ohybu mm 100
Útlum při 600MHz dB/100m 7,8	Celková hmotnost g/m 140
Útlum při 860MHz dB/100m 12	Obsah Cu v kabelu g/m 70
Útlum při 1000MHz dB/100m 13,5	Přenášený výkon při 28MHz kW 2,2
Útlum při 1350MHz dB/100m 15,7	Přenášený výkon při 144MHz kW 0,95
Útlum při 2000MHz dB/100m 20,2	Přenášený výkon při 432MHz kW 0,53
Útlum při 3000MHz dB/100m 24,7	Přenášený výkon při 1296MHz kW 0,31
Průměr vnitřního vodiče mm 2,.62 Cu	Balení m 100

Tabulka 3, konkrétní případ kabelu firmy Belden, H1000 0,22 dB do 3 GHz, a některé udávané parametry dodávané firmou Belden.

Nyní ještě závěrečné slovo ke kabelům. Je velmi důležité zvolit si správný vf kabel. V době plánování spoje víme již, jak bude svod dlouhý a proto si dle dané tabulky 2 - útlumů můžeme spočítat, jak velký útlum svod bude mít. Samozřejmě musíme připočíst i útlum konektorů, bleskojistky, redukcí ale o tom více v kapitole o konektorech.

3.3 - Konektory

Konektory slouží ke spojení vybraného kabelu s WiFi zařízením, s externí anténou a nebo mezi kabely samými. Výběr konektoru je o trochu složitější než výběr kabelu a je nezbytně nutné znát následující údaje:

1) výstupní konektor vašeho WiFi zařízení - nejběžnější je SMA konektor, který se nachází na většině interních PCI karet a *access pointech*. Výjimku tvoří společnosti Avaya a Orinoco, které používají konektor "Mini", či Linksys, který na svých přístupových bodech používá konektor TNC. Je velice důležité zjistit, jestli je konektor samec (*Male*), je opatřen trnem či samice (*Female*), která je opatřena otvorem pro zasunutí trnu samce a dále jestli se jedná o konektor reverzní či nikoli.

2) výstupní konektor na vaší anténě - ve většině případů je použit N konektor ve verzi samice, ale existují i výjimky, kde jsou užity konektory samci.

3) typ vašeho kabelu. Hodně zjednodušeně řečeno jestli bude použit „tenký" nebo „tlustý" kabel pro svod.

Pokud víme všechny potřebné informace o konektorech na WiFi zařízení a anténě, nic nebrání tomu, zakoupení k nim opačných konektorů, kompatibilní s vaším kabelem a vyrobení samotného svodu, jak ilustruji dále. Svody se totiž obvykle z praktických důvodů nevyrábějí, jelikož bývá obtížné táhnout samotný kabel obzvláště s N konektorem ze střechy k WiFi zařízení např. anténním stožárem.

Druhy konektorů:

3.3.1 - N konektory

N konektory jsou robustnější a používají se u namáhaných spojů, snesou větší zatížení, proto se velmi často používají na anténách, díky jejich velikosti se snáze připojují, jsou na nich menší ztráty a snáze se s nimi pracuje.

Jeden z nejčastěji užívaných konektorů VF konektor N-*Male* pro RG-8/LMR-400/RLA-10 a H1000. Zjednodušeně řečeno, N-kový samec na tlustý kabel, používaný k připojení kabelu na anténu je na obrázku 19.

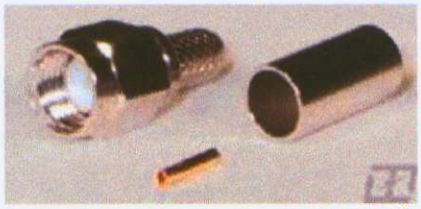
Obr. 19: konektor N-Male pro kabely RG-8/LMR-400/RLA-10 a H1000

3.3.2 - SMA konektory

SMA konektory jsou podstatně menší, používají se většinou u PCI karet, nebo u WiFi zařízení jako jsou hardwarové přístupové body *access point*, čili u zařízení, kde konektor není fyzicky namáhán.

3.3.3 - Reverzní SMA konektory

Konektory velice podobné, konektorům SMA, avšak nestandardní a používané na většině PCI karet a WiFi hardwarových bodech. U reverzního SMA konektoru se jedná o opačné zapojení dutinky a trnu (kolíku) oproti standardnímu SMA konektoru. Proč je tomu tak a proč výrobci preferují právě tyto nestandardní konektory se mi nepodařilo nikde zjistit, ale je poměrně pravděpodobné, že to byl čistě ekonomický kalkul, nutící spotřebitele koupit téměř stejný, avšak až dvakrát dražší konektor než je standardní SMA. Konektor je na obrázku 20.



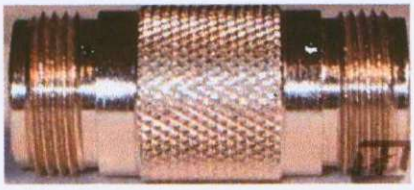
Obr. 20: Konektor reverzní SMA Female - samice

3.3.4 - Lucent konektory

Proprietární konektory firmy Lucent, používané převážně u PCMCIA karet do notebooků. Konektor je opravdu velmi malý, velice citlivý na „špatné zacházení" a velice drahý. Navíc zapojovat ho doma bez sady pro pájení pod lupou je již prakticky nemožné.

3.4 - *Pigtaily* – redukce

Do této kategorie spadají všechny možné redukce z jednoho typu kabelu na jiný (typicky z tenkého RG-58/LMR-195 na tlustý RG-8/LMR-400/RLA-10) nebo z typu jednoho konektoru na jiný. Tyto redukce jsou v praxi poměrně často používané, protože v případě delšího svodu, 10 metrů a více, je vhodnější volit tlustý RLA kabel na jedné straně zakončený konektorem N - *male* a na druhé straně se kabel bude připojovat k malému reverznímu SMA konektoru a proto je dobré použít *pigtail* s reverzním SMA konektorem na tenkém kabelu (RG58) na jedné straně a s N konektorem na druhé straně (není důležité jestli *Male* nebo *Female*). Ten se pak spojí s hlavním svodem. Proč nepřipojit tlustý svod na SMA konektor? Samozřejmě je to možné, dělají se i konektory z tlustého RLA kabelu na reverzní SMA , ale v praxi jsou zdrojem problémů od zapojení tohoto konektoru až po mechanické vylomení konektoru, na který RLA kabel může působit větší sílou než které dokáže drobnější SMA část konektoru vzdorovat.



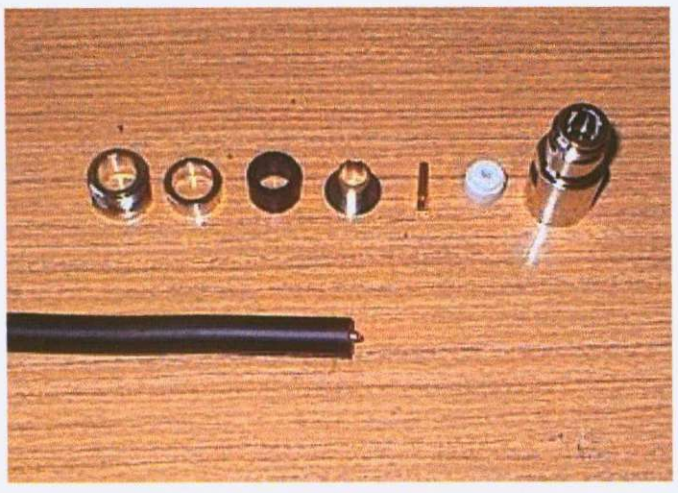
Obr. 21: N samice na N samici

Za povšimnutí na obrázku 22 stojí hlavně poměr velikostí jednotlivých konektorů. Drobný SMA a masivní N konektor.

Obr. 22: Pigtail R-SMA female / N male kabelová redukce

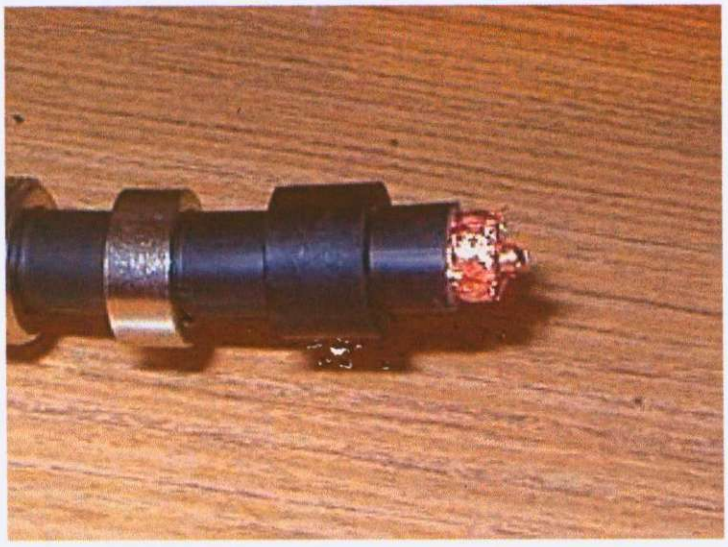
3.5 - Ilustrovaný návod na výrobu N - *Female* konektoru na tlustý RLA kabel

1) Materiál na výrobu osazeného konektoru, obrázek 23.



Obr. 23: Jednotlivé díly konektoru N - Female a RLA kabel

2) Navléknutí zadní části konektoru, ocelové podložky a stahovací gumičky (POZOR velice často, ač se to může zdát k nevíře, se na to zapomíná. U tohoto typu konektoru to sice tolik nevadí, ale u jiných je pak nutné třeba i znova pájet, což je nepříjemné a kabelu to také dobře neudělá.) Seříznutí PVC izolace, 7 mm od začátku vodiče.

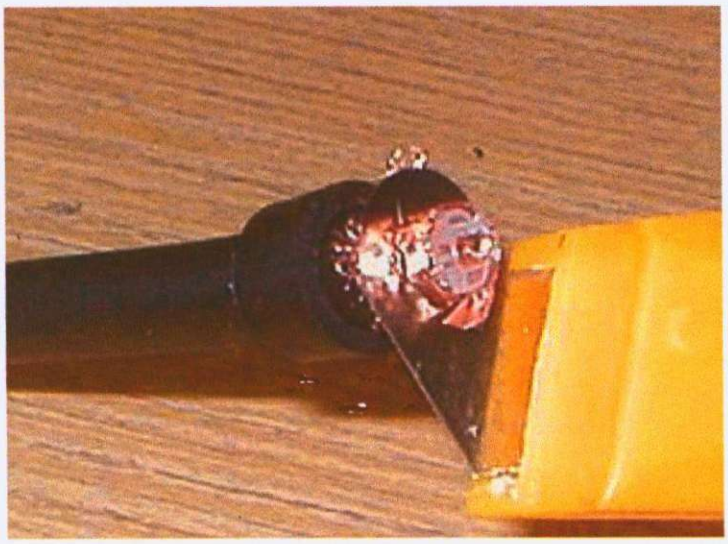


Obr. 24: první krok při výrobě N konektoru.

3) Ohnutí (nesmí se zastřihnout!!!, pouze přiohnout, aby mělo kontakt s podložkou) měděného stínění a zasazení ocelové podložky dle obrázku. Je nutné dát velmi pečlivě pozor, aby se nikde stínění nedotýkalo měděného vodiče.

Obr. 25: vložení podložky

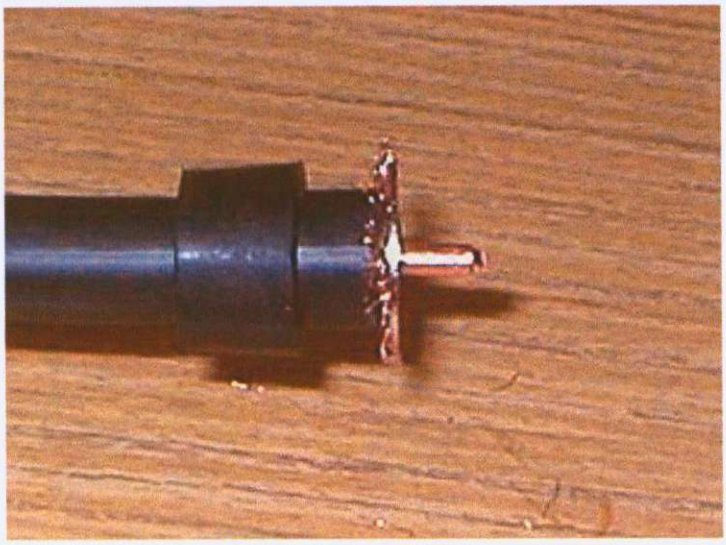
4) Seříznutí izolantu a folie podle podložky, pozor na naříznutí vodiče. Musí zůstat nožem nedotknut.



Obr. 26: seříznutí izolantu

5) Na následující stránce je na obrázku 27 zobrazen vyráběný konektor. V této fázi by měl vyráběný konektor tedy zatím vypadat zhruba takto. Nyní vodič řádně prohřejeme páječkou, naneseme kalafunu a pěkně lehce, ale pravidelně pocínujeme. Do malých kleští uchopíme nasazovaný trn a stejně opatrně nasazovaný vnitřek pokalafunujeme a malinko pocínujeme, stačí opravdu málo, dále se řádně prohřeje cín na vodiči i trnu a sesadí se

dohromady. Zde je třeba být opravdu precizní a věnovat správnému spojení dostatečné a značné úsilí. Trn na vodiči musí pevně držet, musí být přesně v ose s vodičem a cín uvnitř musí být rozprostřen po celém pájeném místě.

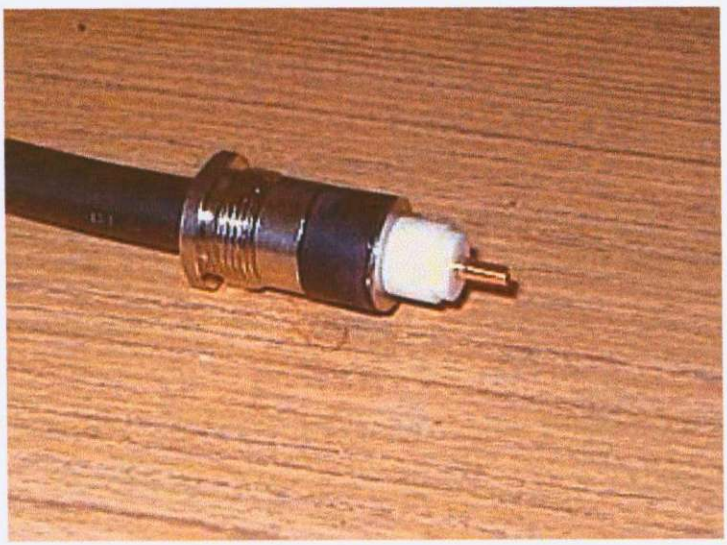


Obr. 27: Kabel připraven k pocínování a připájení Female trubičky.

6) Nyní máme za sebou nejsložitější část výroby konektoru, trn drží na měděném vodiči a celý konektor by měl zatím vypadat jako na obrázku 28.

Obr. 28: Napájená část pevně drží na měděném jádře kabelu.

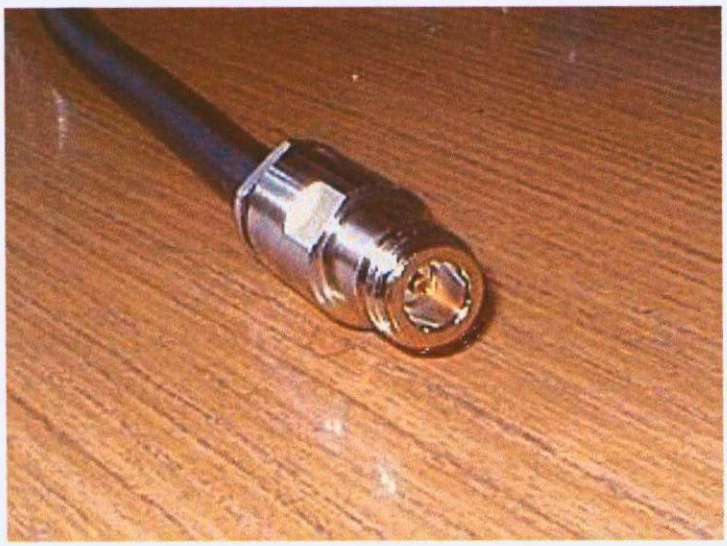
7) Nyní nasadíme izolační teflonové kroužky na trn.



Obr. 29: Nasazení izolačního teflonového kroužku.

8) Nyní nasadíme tělo konektoru a opatrně sešroubujeme (matky na konektoru jsou velikosti 16, takže je potřeba dva klíče této velikosti). Zde pozor, při šroubování se otáčí

pouze zadní částí konektoru, té která je na kabelu, jelikož při otáčení tělem konektoru by se mohl vnitřek a trn poškodit a konektor by nedržel na kabelu pevně. Sešroubovaný konektor je na obrázku 30. Na závěr konektor dle potřeby zaizolujeme, nejlépe nejdříve elektrikářskou PVC izolační páskou a po té vulkanizační páskou. Pokud bude konektor vystaven povětrnostním podmínkám a tudíž dešti, je nutné aby ani v největším dešti do konektoru nezateklo.



Obr. 30: Hotový konektor

Nyní máme VF svod opatřený jedním konektorem a obvykle takto se tedy svod protahuje a druhý konektor se pájí až na místě což bývá nějaká tmavá půda, kde si není ani kam sednout či dokonce kam si pájený konektor položit a celý konektor se pájí v ruce v těchto polních podmínkách se teprve vyplatí být co nejpreciznější a velice velice trpělivý.

3.6 - Ilustrovaný návod na výrobu krimpovacího SMA reverzního *Female* konektoru na tenký LMR 195 kabel

1) Pomocí krimpovacích kleští lze udělat konektor bez pájení, ale mnohem spolehlivější je konektor i tak pájet.

Obr. 31: Krimpovací kleště

2) Zde jsou na obrázku 32 dva SMA konektory, SMA *Male* a SMA reverzní *Female*. Jak je vidět, rozdíl mezi nimi je pouze *Male* u trn a u *Female* trubička.

Obr. 32: SMA Male a SMA reverzní female konektory

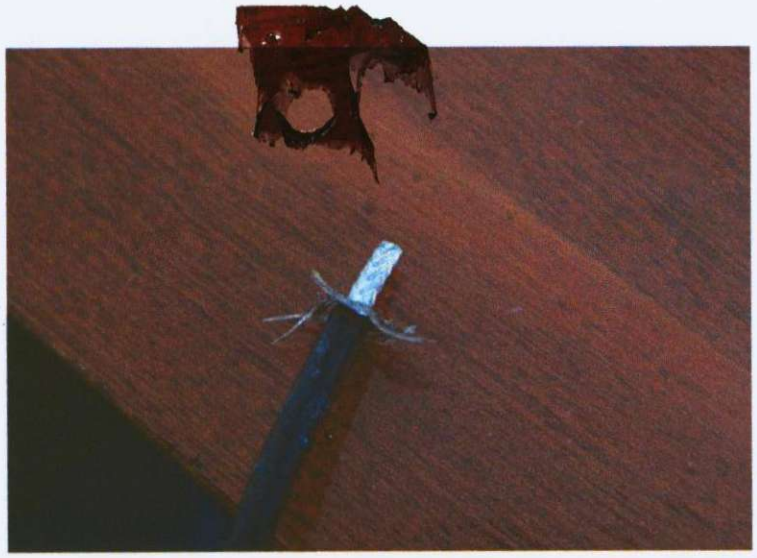
3) Tenký kabel LMR 195 a první, krok výroby konektoru, nasazení krimpovací objímky na kabel.

Obr. 33: LMR 195

4) Odstranění svrchní izolace ve vzdálenosti 13 mm od začátku kabelu. Pod izolací je vidět stínění kabelu.

Obr. 34: LMR 195 - stínění

5) Přiohnutí stínění od kabelu.

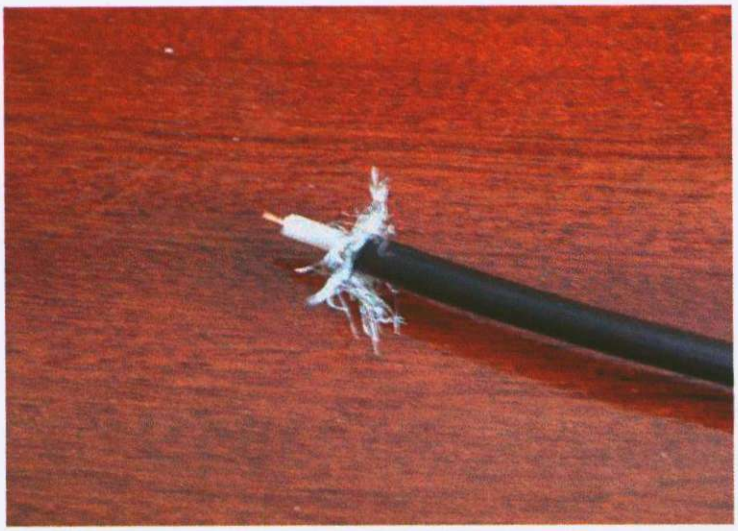


Obr. 35: Přihnuté stínění kabelu.

6) Odstranění hliníkové folie

Obr. 36: Kabel LMR 195 s odstraněnou hliníkovou folií

7) Ostrým nožíkem nebo skalpelem se opatrně seřízne teflonový izolant 3 mm od začátku kabelu. Značný důraz je třeba klást na nepoškození měděného jádra kabelu – vodiče.



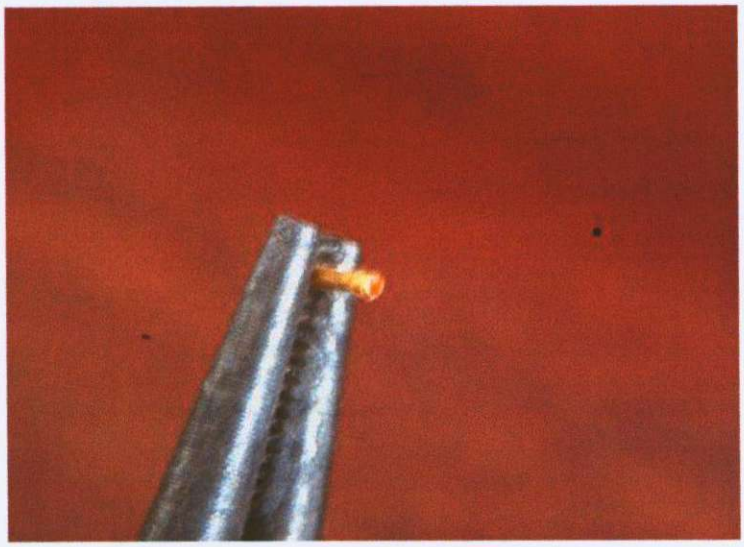
Obr. 37: LMR 195 - Měděné jádro

8) Nanesení kalafuny a řádné pocínování jádra. Zde je třeba dbát na opravdu rovnoměrné pocínování a dávat pozor na izolant, který je na teplo poměrně citlivý a při větší teplotě dochází k protavování měděného jádra ze středu kabelu, což je samozřejmě nežádoucí. Jádro musí zůstat stále na stejném místě, uprostřed kabelu.

Obr. 38: Pocínování měděného jádra kabelu

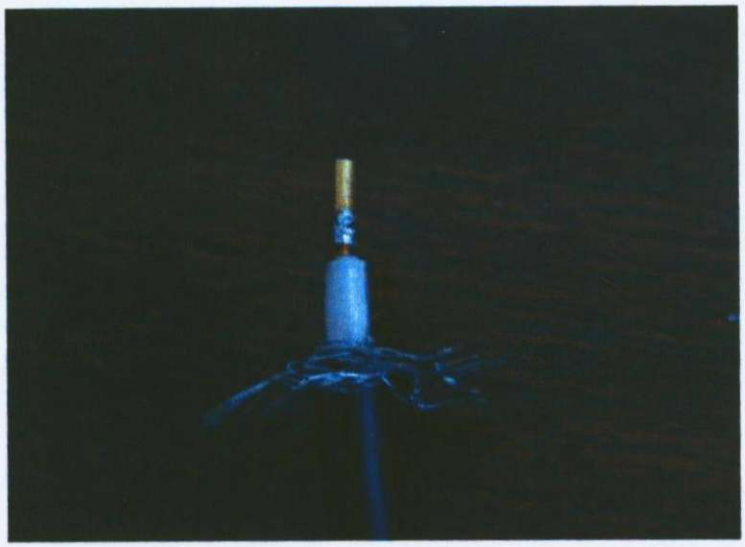
9) Nyní nastává nejsložitější část výroby konektoru a sice nasazení a napájení trubičky

resp. trnu u *Male* konektoru. Trubička, resp. trn se uchopí malými kleštěmi, jak je vidět na obrázku 39, páječkou se prohřeje a na vnitřek, který se bude nasazovat na měděné jádro, se nanese kalafuna, aby se na vnitřek trubičky, resp. trnu chytal dobře cín. V praxi je to docela složitá operace a obzvláště je-li prováděna v „polních" podmínkách někde na půdě je třeba dobře zacházet s páječkou. Jinak je dobré si kabel uchytit, např. do svěráku, aby „neutíkal", ale nesmí se příliš sevřít aby nebyli porušeny jeho parametry.



Obr. 39: Příprava na pocínování a nasazení trubičky konektoru

10) Napájená část se zbaví přebytkového cínu a řádně prozkouší zda je pevně a kvalitně připájena.



Obr. 40: LMR 195 a část SMA konektoru

11) Nyní se velice opatrně nasadí tělo konektoru. U konektorů *Female* je třeba dávat obzvláště velký pozor při nasazování, trubička je malá a velice měkká a snadno se zláme když se nenasazuje zcela přesně v podélné ose konektoru do předvrtaného otvoru. Opravdu je třeba být velice důkladný a zbytečně nespěchat. Nemá cenu zničit konektor ve fázi kdy je již téměř hotov.

Obr. 41: Nasazená konektor SMA reverzní Female.

12) Obtočit stínění kabelu kolem těla konektoru v místě k tomu určeném. Stínění je třeba

tak o 3 - 4 mm zkrátit. V této části výroby svodu je též vhodné si kabel proměřit elektroměrem proti zkratováním. Konektor nesmí vést elektrický proud mezi celým tělem konektoru a trubičkou, resp. trnem v konektoru. Pakliže tomu tak není, konektorem projde elektrický proud, konektor je zkratován a je třeba tělo konektoru sundat, pečlivě prohlédnout jestli se drobný drátek stínění někde nedotýká, či není někde jiné elektrické propojení, znovu nasadit tělo konektoru a změřit.

Obr. 42: Téměř hotový konektor - stínění obtočeno kolem konektoru

13) Nyní již zbývá pouze nasadit krimpovací objímku...

Obr. 43: Téměř hotový konektor připraven na namáčknutí krimpovacími kleštěmi

14) Zmáčknout krimpovacími kleštěmi...

Obr. 44: Krimpovací kleště při práci

15) ... a konektor je hotov. Pro venkovní použití se po spojení s konektorem antény musí utěsnit samovulkanizační páskou, aby se do konektorů nedostala voda a vysokofrekvenční

svod je hotov.

Obr. 45: Hotový konektor SMA reverzní Female

Na a závěr této kapitoly o VF svodu, bych tedy ještě problematiku malinko shrnul. Kabel od antény k WiFi zařízení je speciální vysokofrekvenční kabel a s jako takovým je třeba zacházet. Kabely se dají rozdělit do spousty kategorií, ale v rámci zjednodušení vhodného do praxe bych kabely rozdělil na „tlusté a tenké", čili nízkoútlumové RG-8/LMR-400/RLA-10 (tlusté) a RG-58/LMR-195 (tenké). Konektorů k WiFi zařízením a anténám je opět několik druhů ale ty nejpoužívanější jsou N konektor a reverzní SMA. Konektory se připojují na „tlustý nebo tenký" kabel a podle toho jsou též označovány. Tedy například VF konektor SMA reverzní - *Female* pro RG-58/LMR-195 je reverzní SMA samice a tento konektor se pájí na tenký kabel. Analogicky se pojmenovávají ostatní konektory. [1, 3, 5]

3.7 - Vlastní WiFi zařízení - transciever

Závěrem se dostáváme k samotnému WiFi zařízení. WiFi zařízení je dneska již nepřeberné množství, ale já pohled malinko zredukuji pouze na zařízení používaná pro připojení PC do počítačové sítě. Ptáte se k čemu se tak asi může WiFi ještě jinému používat? Jak jsem již psal na začátku práce, technologie WiFi zažívá opravdový *boom*, a používá se stále častěji pro přenos dat nejen mezi počítači, ale stále více mezi periferiemi

3.7.2 - Mini-PCI integrované moduly

Čím dál větší skupina nových notebooků i stolních počítačů i kapesních počítačů (PDA) přichází od výrobce s integrovaným Mini-PCI WiFi rádiem (či je WiFi již součástí chipové sady). To jenom potvrzuje budoucnost bezdrátových sítí a to, že dříve nebo později bezdrátové sítě v určitých sektorech naprosto nahradí klasické drátové ethernetové sítě.

Obr. 47: Mini-PCI integrovaná karta

3.7.3 - USB adaptéry

Většina stolních počítačů nemá slot pro PCMCIA karty. Tento problém můžete vyřešit použitím PCI/ISA adaptérů nebo USB WiFi adaptérů. Pro velký počet uživatelů používajících stolní počítače je nejjednodušší cestou, jak přidat WiFi rádio, použít USB adaptér. Není nic jednoduššího než připojit adaptér do USB konektoru počítače a pokračovat v instalaci ovládacího softwaru a příslušných ovladačů dodaných výrobcem. V případě instalace na počítač s Windows XP platí podobně jako u PC karet, že ovladače a potřebný software může být již obsažen v operačním systému. USB adaptéry jsou paradoxně cenově o trochu výše než PC karty. Jejich ceny se pohybují od 2,500 Kč výše (podzim 2005). Prodejci v České Republice jsou především Elity, ZCOMAX, ASM, LEVI, i4 a další.

3.7.4 - Přístupové body (*access pointy*) a brány

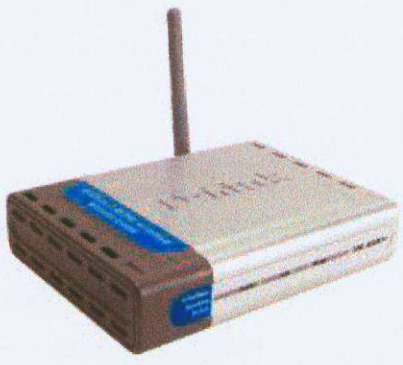
Další skupinou o které se zde zmíním jsou přímo hardwarové zařízení, též se jim říká *access pointy* (AP) resp. brány, ačkoliv pojmenování *access point* je poněkud nepřesné a bere se v užším slova smyslu. V širším slova smyslu je *access point* technické zařízení používané jako server k připojení bezdrátových klientů. Tyto hardwarové zařízení se dělí ještě na několik druhů, brány a přístupové body a jejich kombinace. Rozdíly mezi nimi nemusí být tak zřetelné, protože jejich funkce se mohou překrývat.

Bezdrátová brána (*gateway*) je užívána především v prostředí plně bezdrátových sítí v domácnostech nebo menších firmách. Přístupový bod (*access point*) je více užíván v prostředí kombinovaných sítí bezdrát-LAN větších rozměrů. Brány a přístupové body mohou být rozdílné v otázkách kapacity, zabezpečení, řízení síťové komunikace, atd. Brány často podporují NAT (Network Address Translation) routování a DHPC (Dynamic Host Control Protocol) služby. Ty umožňují tvorbu jednotlivých IP adres, které klientská zařízení potřebují k tomu, aby pracovala v síti. WiFi brána většinou zajišťuje připojení všech klientů sítě k jedné internetové přípojce. Brány také mohou obsahovat aplikace na řízení zabezpečení, šifrování, VPN, *firewall* a VoIP. Abych to pro porozumění zjednodušil, toto zařízení má jako LAN (Local Area Net) port WiFi, ke kterému se připojují bezdrátoví klienti a WAN (Wide Area Net) port bývá většinou standardní ethernet rozhraní připojované konektorem RJ-45, ale není podmínkou, možno je i DSL připojení, ISDN a další.

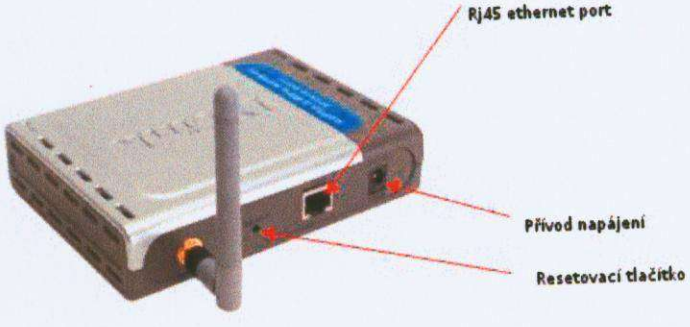
Přístupové body (*access pointy*) nepodporují NAT *routování* či DHPC. Tyto funkce jsou většinou zajišťované routry zapojenými dále. Přístupové body pracují jako mosty mezi "drátovou" ethernetovou sítí typu LAN a klienty připojenými bezdrátově. Přestože přístupové body obecně nepodporují NAT nebo DHPC, umožňují *roaming* (možnost přecházet z jednoho přístupového bodu na druhý bez ztráty spojení se sítí), vyšší stupeň zabezpečení, lepší kontrolu a řízení sítě. Některé brány mohou také podporovat tyto služby. Obecně vzato mnoho bezdrátových základnových stanic může pracovat jako přístupový bod nebo brána, záleží jen na nastavení.

Tedy opět pro zjednodušení a porozumění. Toto zařízení obvykle pracuje přesně opačně než první zmíněné. Dalo by se říci, že jeho WAN port, tedy část připojující do sítě je právě bezdrátová část a LAN je tradičně ethernet do lokální sítě, za kterým následuje síťový přepínač, tak zvaný *switch* nebo, ještě častěji *router* pro oddělení sítí a *switch* je až za ním. Samozřejmě záleží na nastavení, přístupový bod může (paradoxně právě díky jeho

menšího funkčního vybavení) pracovat i obráceně, ale to si vše ukážeme na příkladu konfigurace typického představitele přístupových bodů firmy D-Link® DWL-900AP+.



Obr. 48: DWL-900AP+



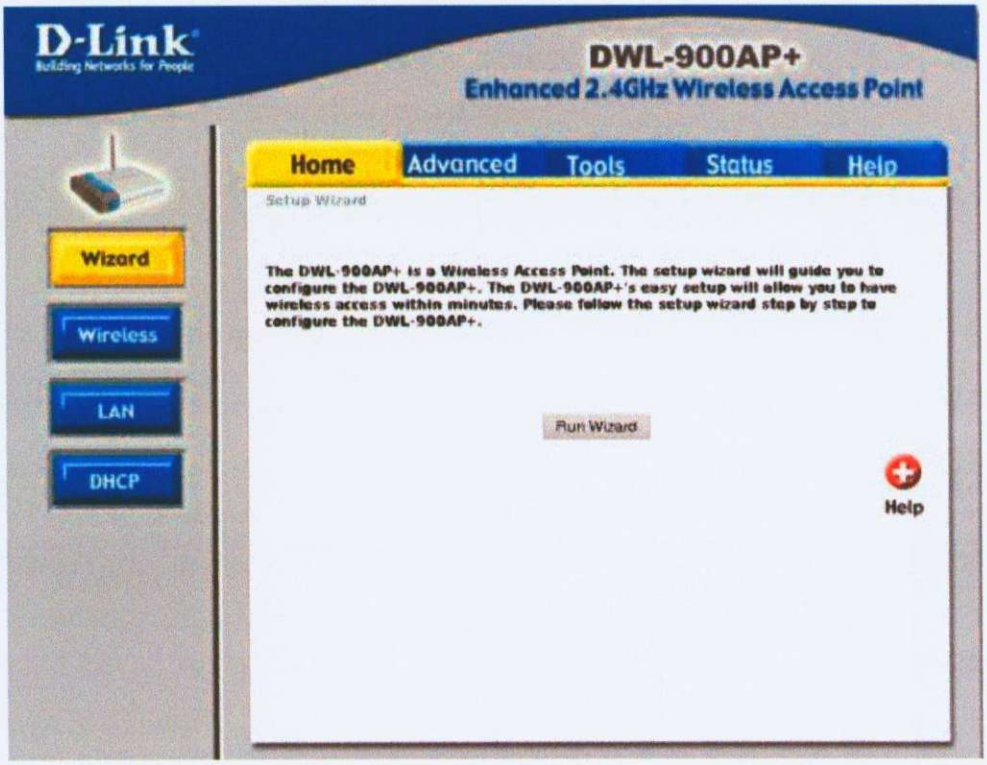
Obr. 49: DWL-900AP+ - zadní strana

3.7.4.1 - Konfigurace DWL-900AP+

Připojíme si AP k počítači (Pozor, pokud spojujete zařízení UTP kabelem přímo k počítači, je třeba křížený kabel, na PC si nastavíme IP adresu na 192.168.0.2, spustíme www prohlížeč a do řádky na URL napíšeme přednastavenou IP adresu AP, která je 192.168.0.50

Vyskočí okno s přihlašovacím jménem které je: admin a heslo k přístupu, které není žádné.

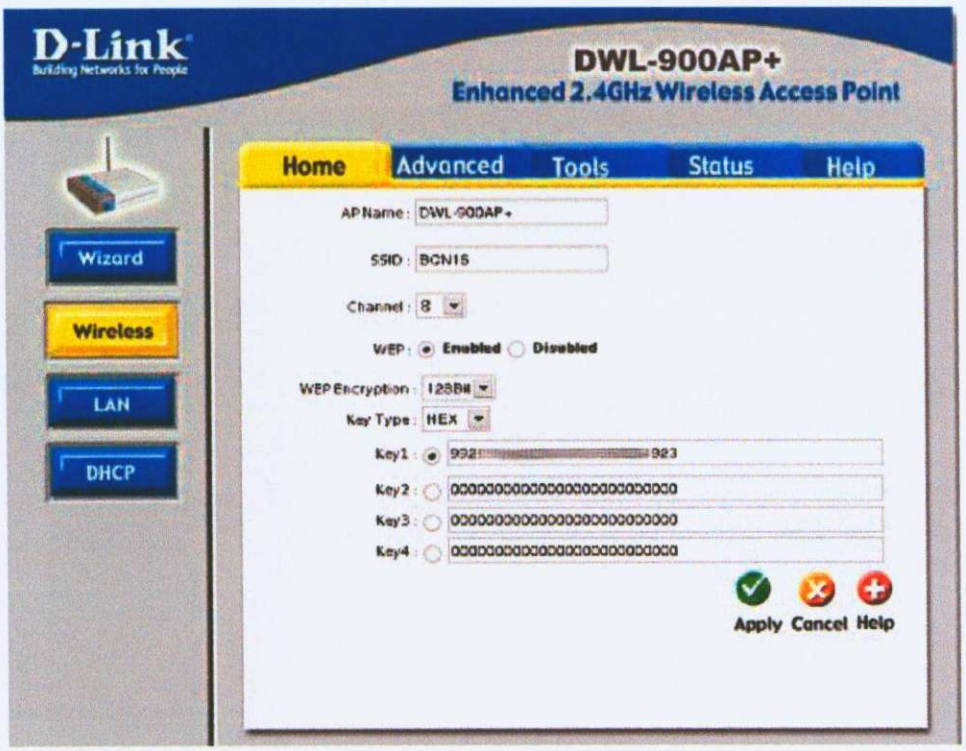
Na následující stránce je úvodní obrazovka po přihlášení:



Obr. 50: Hlavní stránka www konfiguračního rozhraní DWL-900AP+

Jako první je dobré nastavit si bezdrátovou část zařízení a část ethernetovou udělat až zcela nakonec, protože při změně IP adresy zařízení se musí změnit i IP adresa počítače ze kterého konfigurujeme přístupový bod, protože jinak se přístupový bod může octnout v jiné síti a pak se samozřejmě nebude možné se na něj z důvodu směrování paketů v IP síti připojit. Na obrázku 51. je základní nastavení parametrů pro bezdrátovou část. První je jméno AP, zde vyplníme libovolné jméno, které si vybereme, na provoz nemá žádný vliv.

Další políčko obsahuje již důležité SSID (service set identifier), v našem případě BCN15, což je jméno *access pointu* ke kterému se zařízení přihlašuje v režimu klient, nebo jméno *access pointu* v režimu Access Point, který si nastaví klienti tohoto zařízení když se na něj chtějí připojit a komunikovat přes něj. Kanál nám říká na kterých frekvencích má zařízení pracovat a volba wep je pro zapnutí – enabled či vypnutí – disabled šifrování WEP sloužící k zabezpečení provozu. O bezpečnosti více v kapitole 4. Jestli zvolit 64bitový klíč či 128bitový klíč již záleží zcela na požadavcích na zařízení, ale obecně platí čím delší šifrovací klíč, tím bezpečnější. Pokud je tedy šifrování WEP povoleno, musíme zadat klíč a to buď ve formě hexadecimální – šestnáctkové číslo, nebo ASCII...Opět pokud je zařízení v modu klient či Access Point, klíč se použije podle toho buď k přístupu na jiné zařízení nebo když zařízení pracuje v modu Access Point jako restrikční činitel pro ostatní zařízení přihlašující se do sítě. Jelikož se tomto případě jedná o skutečné, běžící AP, je z bezpečnostních důvodů hodnotu klíče rozmazána.



Obr. 51: Základní konfigurace bezdrátové části DWL-900AP+

Dále je nutné nastavit pokročilé parametry bezdrátové sítě. U většiny *access pointů* se nastavují ty samé hodnoty, snad jen graficky se konfigurační www rozhraní jednotlivých výrobců liší.

Na tomto obrázku je vidět seznam módů ve kterých je možné *access point* provozovat. Nás ale zajímají hlavní dva tj. mód Access Point a mód Wireless Client. Co který dělá je zcela zřejmé z jejich názvů a myslím že není již potřeba se vracet k vysvětlování. Snad jen malá poznámka právě k výrobku DWL-900AP+, který má jednu velkou výhodu (nejen on) v tom, že se mu v mód Wireless Client nemusí zadávat MAC adresa přístupového bodu, stačí pouze jeho název a místo MAC adresy nuly, jak je vidět na obrázku. A proč že je to taková výhoda? Představme si přístupový bod, se kterým je asociováno 20 takovýchto klientů a nyní si představme, že tento přístupový bod přestane fungovat a je třeba ho vyměnit. Ano, kdyby byli bezdrátoví klienti asociováni dle MAC adresy, na všech by se musel přenastavovat přístupový bod. Takto to není třeba.

Ještě jednu věc bych rád zdůraznil, a sice tlačítko Site Survey. Toto tlačítko proscanuje okolí a najde možné přístupové body.

Poznámka: DWL-900AP+ mají malou chybu ve firmwaru a po kliknutí na tlačítko Site Survey je nutno ve www prohlížeči znovu načíst stránku. Bez tohoto se nic nezobrazí.

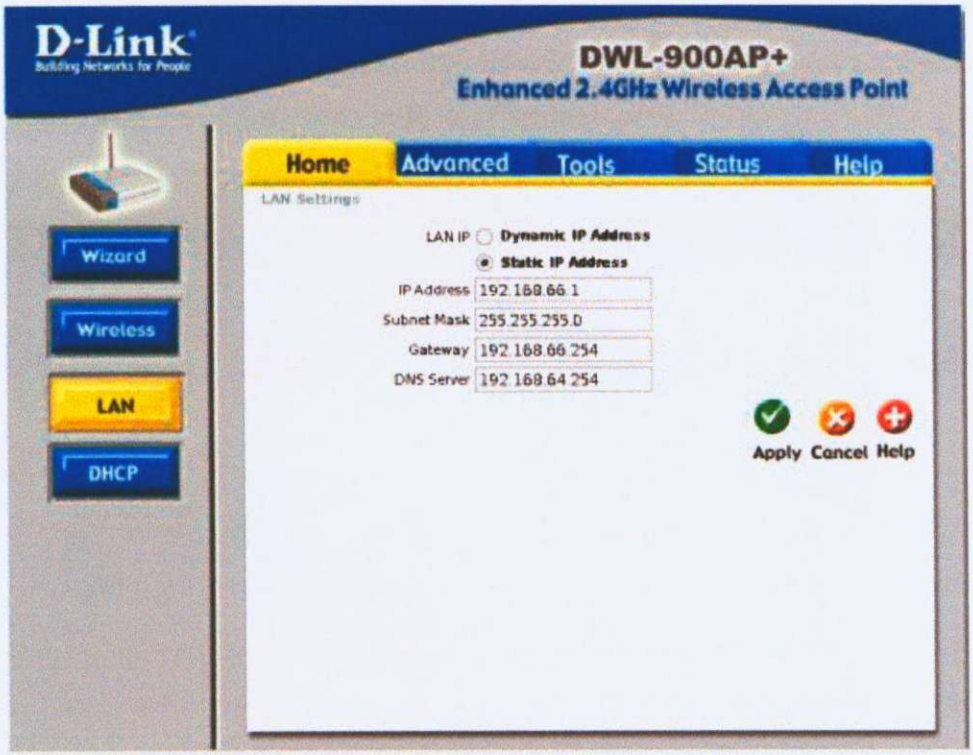
Obr. 52: Pokročilé rozhraní konfigurace bezdrátové části DWL-900AP+

Nyní k dalším módům *access pointu*. Wireless Bridge. V tomto módu *access point*

pouze předává veškerý provoz z jednoho portu na druhý. Více si o tomto režimu ještě napíšeme v kapitole o PCI kartách při jejich nastavování v Linuxu.

Repeater. Repeater je v podstatě zesilovač. Přijme signál a odešle jej zvětšený na velikost svého výkonu. Tím odešle signál dále. V praxi se mód *repeater* často nepoužívá vzhledem k zarušení prostředí a režii IP protokolu s tím spojenou.

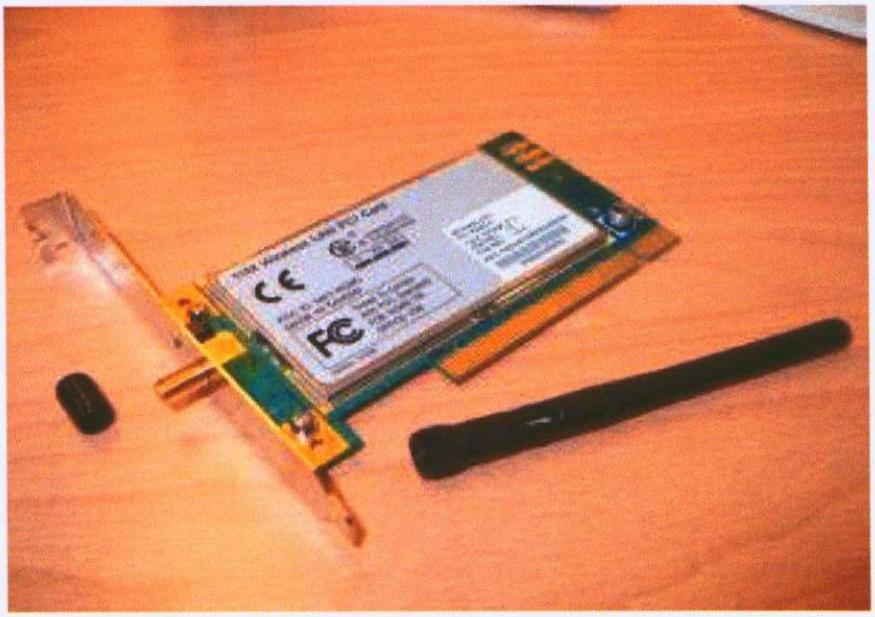
Na obrázku 53 Je vidět konfigurace ethernetového rozhraní *access pointu.* Opět platí, že většina těchto zařízení od různých výrobců má stejné nebo velmi podobné volby nastavení. Jak také jinak, protokol IP je zcela jasně definován a aby zařízení tímto protokolem mohlo komunikovat, musí mít nastaveny právě tyto čtyři volby. IP adresu, která přiřazuje jedinečné jméno zařízení v dané síti, masku sítě, která doplňuje informaci o zařazení zařízení do sítě, *gateway* na kterou se směřují odchozí pakety a adresu jmenného serveru DNS, který provádí překlad jmenných adres, lépe srozumitelných člověku na IP adresy, která ale pro činnost samotného zařízení potřeba není.[10]



Obr. 53: Konfigurace ethernetové části DWL-900AP+

3.7.5 - PCI / ISA interní adaptéry

Mnoho výrobců bezdrátových zařízení dodává WiFi rádia ve formě PCI nebo ISA interních karet pro stolní počítače, které umožní připojení počítače k bezdrátové síti. Tyto karty jsou buď PCI/ISA karty s otevřeným slotem pro vložení WiFi rádia ve formě PCMCIA karty a nebo PCI/ISA karty s integrovaným WiFi rádiem. Některé modely mají výstup i na externí anténu, což jim umožňuje příjem a vysílání signálu od/do vzdálenějšího zdroje a o těch bych rád promluvil obšírněji. Opět je více druhů těchto karet, co výrobce to druh, ale je třeba zdůraznit, že většina výrobců do svých karet dodává již dalo by se říci standardní *chipsety* a pouze „okolo nich vystaví" kartu a nalepí na ní nálepku se svým logem. Nejznámější *chipsety* jsou Atheros 52xx, Prism 2.5, Prism 2, Orinico/Agere/Hermes, ADMtek 8211, ale i firma intel má svůj chipset Intel 2200 a další. Já se zde zaměřím na chipset Prism 2,5, protože tento *chipset* je plně podporován operačním systémem GNU Linux a pomocí něj se dají s kartou vybavenou tímto *chipsetem* , nejčastěji Zcom XI-626 provádět nejsložitější síťové funkce, které právě operační sytém GNU Linux zastává na výbornou, navíc ještě za příjemnou cenu.



Obr. 54: XI-626

Většina operačního systému GNU Linux je dodávána pod licencí GPL (General Public Licence), přesné znění lze najít na internetové adrese: http://www.gnu.org/copyleft/gpl.html. Zjednodušeně licence říká, že se s programovým zdrojovým kódem dá dělat cokoliv, po libosti ho měnit, upravovat, poté i prodávat, ale musí se vždy dodávat se zdrojovými kódy. V praxi to ale vypadá tak, že většina software vydaná s licencí GPL je zdarma. Pozor, není to ale podmínkou a velké množství uživatelů si toto stále plete.

3.7.6 - WiFi PCI karty a operační systém GNU Linux

3.7.6.1 - Příprava počítače

Nyní si zde podrobněji popíšeme konfiguraci linuxového přípojného bodu. Co budeme potřebovat? O Linuxu je známo, že dokáže běžet i na mnohem slabším hardware, než například operační systémy firmy Microsoft a jedním z důvodů proč tomu tak je, je maximální možná optimalizace na hardware na kterém Linux běží, která je dána právě zdrojovými soubory jádra operačního systému, tzv. kernelu, který se zkompiluje přímo na daný hardware. Pokud chceme docílit ještě dalšího urychlení běhu systému, spíše by se dalo říci maximálního „vyždímání", je možné instalovat celý systém ze zdrojových souborů, což může být poměrně časově náročné a složité. Obojího – složitosti i časové náročnosti se ale můžeme zbavit jednou vhodnou volbou a sice linuxovou distribucí Gentoo linuxu. Linuxová distribuce Gentoo zdrojová distribuce, to znamená, že se celý systém instaluje ze zdrojových balíčků, takzvaných ebuildů, které si hlídají závislosti, čím nám právě velice usnadní instalaci.

K instalaci tedy potřebujeme nějaký starší hardware architektury nejlépe x86 (procesory Intel a kompatibilní), kterého jsou na základních školách plné učebny. Pro hardware platí jednoduché pravidlo, a sice čím složitější síťové operace chceme na stroji provádět, tím potřebujeme lepší stroj. Pokud potřebujeme pouze jednoduše *routovat*, stačí po49ta4 s procesorem Intel kompatibilní řádu 486 s 4MB ÷ 8 MB operační paměti,pokud ale potřebujeme *firewall* – paketový filtr, QoS, *shaping* – rozdělení konektivity dle určitých pravidel jednotlivým uživatelům, *HTB, IMQ* s desítkami pravidel, potřebujeme již silnější hardware. V našem případě, vytvoření jednoduchého přístupového bodu a klienta, stačí počítač s procesorem Intel Celeron s taktem 200 MHz ÷ 400 MHz a od 16 MB operační paměti výše. Dále potřebujeme dvě karty XI-626 a libovolnou distribuci Linuxu.

Do počítače vložíme karty a nainstalujeme Linux. Jestli použijeme distribuci Redhat, Slackware, Debian není důležité, důležité je vědět že není potřeba instalovat grafické rozhraní, tak zvaná Xka, ani žádný okenní manager. Pokud instalujeme distribuci Gentoo, je třeba stáhnout si z internetové adresy http://www.gentoo.org/main/en/where.xml minimální cd image, nabootovat a držet se perfektně napsaného návodu z adresy: http://www.gentoo.org/doc/en/handbook/handbook-x86.xml. Ještě zdůrazním jednu možnost a tou je distribuovaný překlad distcc. Tato volba se použije při překládání celého systému na starém stroji, kde by překlad trval i několik dní a funguje tak, že se tento stroj umístí do počítačové sítě, kde na každém počítači je distcc klient a na našem instalovaném je distcc server a při překladu si počítače vypomáhají. Toto je takový zjednodušený výpočetní cluster. Více informací o distcc je na adrese: http://www.gentoo.org/doc/en/distcc.xml.

Takže nyní máme již nainstalovaný počítač s Linuxem a zbývá nám nakonfigurovat WiFi karty. K tomu je zapotřebí několika věcí. Jádro starší 2.4.21 a v něm zakompilované wireless extensions > 15 (WE15), aktuální ovladače hostap z http://hostap.epitest.fi/ a nejnovější wireless tools z

http://pcmcia-cs.sourceforge.net/ftp/contrib/. Z http://www.kernel.org stáhneme nejnovější jádro, nyní linux-2.6.10.tar.bz2 a zkopírujeme do adresáře /usr/src/ .

Poznámka: root@Puda:~# je výpis konzole bashe, který říká, že jsme přihlášeni na počítači se jménem Puda jako superuživatel root. Příkaz je tedy až za tímto promptem.
root@Puda:~#cp linux-2.6.10.tar.bz2 /usr/src

, přepneme se do adresáře

root@Puda:~#cd /usr/src

rozbalíme,

root@Puda:~#tar -xvjf linux-2.6.10.tar.bz2

vytvoříme symbolický link /usr/src/linux,

root@Puda:~#ln -s linux-2.6.10 linux

a přeložíme jádro. Opět musím říci, že je dalece nad rámec této práce popisovat kompilaci kernelu, proto pouze vložím několik odkazů na návod v češtině, kde je kompilaci jádra věnována patřičná pozornost.

http://www.abclinuxu.cz/clanky/navody/cesta-do-hlubin-kompilace-jadra-1

http://www.abclinuxu.cz/clanky/navody/cesta-do-hlubin-kompilace-jadra-2-hardware

http://www.abclinuxu.cz/clanky/navody/cesta-do-hlubin-kompilace-jadra-3

nebo

http://www.abclinuxu.cz/clanky/navody/kompilovanie-jadra-i

http://www.abclinuxu.cz/clanky/navody/kompilovanie-jadra-ii

Je třeba do jádra přeložit používání iptables a všechny jeho volby jako moduly (volba „M" u požadované položky).

Když je jádro přeložené a nabootované, zbývá ještě stáhnout a přeložit ovladač hostap. Překládá se velice jednoduše, nejdříve soubor rozbalíme:

root@Puda:~#tar -xzvf hostap-driver-0.3.9.tar.gz

(poslední aktuální verze – listopad 2005)

přepnout se do adresáře s ovladačem:

root@Puda:~#cd hostap-driver-0.3.9

zkompilovat

root@Puda:~#make pci

a instalovat

root@Puda:~#make install_pci.

Tímto se vytvoří jaderný modul hostap_pci a hostap_crypt, který se musí s každým startem systému zavádět do jádra. Pro uživatele neznalé Linuxu je nejjednodušší do souboru /etc/conf.d/local.start. Je možné že se soubor local, též rc.local nachází i jinde, ale vždy je možné ho nalézt v některém z podadresářů adresáře /etc/.

modprobe hostap_pci

modprobe hostap_crypt

Poznámka: soubor rc.local či local.start je ve všech linuxových distribucích. Je to skript, který se spouští jako poslední při startu systému ve všech startovacích *runlevelech.*

Zavedením těchto modulů se nám vytvoří dvojice zařízení wlan0 a wifi0, resp. wlan1, wifi1 a pokud bude WiFi karet více, tak i další, číslované inkrementálně dále. Obě zařízení se stejným číslem jsou totožná a zařízení wifi0 jsou zde pouze pro kompatibilitu s BSD systémy.

dále rozbalíme a přeložíme wireless tools:

root@Puda:~# tar -xzvf wireless_tools.27.tar.gz

(poslední aktuální verze – listopad 2005)

root@Puda:~#cd wireless_tools.27

root@Puda:~#make

root@Puda:~#make install

V adresáři /usr/local/sbin jsou přeloženy utility pro ovládání WiFi karet. Teď zkontrolujeme jestli máme adresář /usr/local/sbin v systémové proměnné $PATH. To uděláme takto:

root@Puda:~#echo $PATH

/sbin:/bin:/usr/sbin:/usr/bin

Zde adresář /usr/local/sbin není a tak to napravíme a na začátek souboru /etc/conf.d/local.star zapíšeme toto:
export PATH=$PATH:/usr/local/sbin
restartujeme počítač a vyzkoušíme echo $PATH.

Pro nás nejdůležitější je iwconfig, který nastavuje všechny nám potřebné parametry. Pouhé spuštění příkazu iwconfig nám ukáže nastavení karet.
root@Puda:~# /usr/local/sbin/iwconfig

lo no wireless extensions.

wlan0 IEEE 802.11-b ESSID:"STARNET_122"

Mode:Managed Frequency:2.422GHz Access Point: 00:11:D8:CB:E0:DC

Bit Rate:1Mb/s Tx-Power=20 dBm Sensitivity=1/3

Retry min limit:8 RTS thr:off Fragment thr:off

Encryption key:7855-3285-72 Encryption mode:restricted

Power Management:off

Link Quality:58/92 Signal level:-66 dBm Noise level:-100 dBm

Rx invalid nwid:0 Rx invalid crypt:673541 Rx invalid frag:9

Tx excessive retries:2423397 Invalid misc:87353353 Missed beacon:0

wifi0 IEEE 802.11-b ESSID:"STARNET_122"

Mode:Managed Frequency:2.422GHz Access Point: 00:11:D8:CB:E0:DC

Bit Rate:1Mb/s Tx-Power=20 dBm Sensitivity=1/3

Retry min limit:8 RTS thr:off Fragment thr:off

Encryption key:7855-3285-72 Encryption mode:restricted

Power Management:off

Link Quality:58/92 Signal level:-66 dBm Noise level:-100 dBm

Rx invalid nwid:0 Rx invalid crypt:673541 Rx invalid frag:9

Tx excessive retries:2423397 Invalid misc:87353353 Missed beacon:0

wlan1 IEEE 802.11-b ESSID:"DOBRA_VODA"

Mode:Master Frequency:2.422GHz Access Point: 00:11:D8:CB:E0:E2

Bit Rate:11Mb/s Tx-Power=20 dBm Sensitivity=1/3

Retry min limit:8 RTS thr:off Fragment thr:off

Encryption key:1921-3334-72 Encryption mode:restricted

Power Management:off

Link Quality:58/92 Signal level:-66 dBm Noise level:-100 dBm

Rx invalid nwid:0 Rx invalid crypt:673541 Rx invalid frag:9

Tx excessive retries:24097 Invalid misc:873123 Missed beacon:0

wifi1 IEEE 802.11-b ESSID:"DOBRA_VODA"

Mode:Master Frequency:2.422GHz Access Point: 00:11:D8:CB:E0:E2

Bit Rate:11Mb/s Tx-Power=20 dBm Sensitivity=1/3

Retry min limit:8 RTS thr:off Fragment thr:off

Encryption key:1921-3334-72 Encryption mode:restricted

Power Management:off

Link Quality:58/92 Signal level:-66 dBm Noise level:-100 dBm

Rx invalid nwid:0 Rx invalid crypt:673541 Rx invalid frag:9

Tx excessive retries:24097 Invalid misc:873123 Missed beacon:0

eth0 no wireless extensions.

Nyní si popíšeme podrobně celý soubor /etc/conf.d/local.start. Aby se dal použít přímo tento pouhým okopírováním z diplomové práce, doplním ho komentáři. Komentář je v interpretru bash vše co je za znakem #.

3.7.6.2 - Konfigurační soubor /etc/conf.d/local.start

root@Puda:~# cat /etc/conf.d/local.start

#!/bin/sh

#Každý bash skript musí začínat tímto #!/bin/sh a říká se tím příkazovému interpretru, že
#se jedná o dávkový soubor, a že se má zpracovat interpretrem bash.

/etc/conf.d/local.start: Local system initialization script.

#

Put any local setup commands in here:

modprobe 3c59x

modprobe hostap_pci

modprobe hostap_crypt #Načtení modulů-ovladačů pro ethernetovou kartu 3Com 3c59x a
WiFi karet

iwconfig wlan0 channel 3 #nastevení karty na třetí kanál

iwconfig wlan0 mode managed #nastavení karty do režimu klient

iwconfig essid STARNET_122 #připojení na AP STARNET_122, pozor ve jménu AP se
#rozlišují velká a malá písmena, proto STARNET_122 a starnet_122 jsou zcela jiné AP

iwconfig wlan0 key 7855328572 #Přístupový bod je chráněn před nežádoucím připojením
#pomocí WEP klíče. Toto je zadání WEP klíče.

iwconfig wlan0 txpower 10 # Veliká přednost linuxového AP, takto se nastavuje vysílací
#výkon karty, ale o tom si povíme ještě podrobněji dále.

iwconfig wlan1 channel 8

iwconfig wlan1 mode master #Nastavení druhé karty do režimu AP

iwconfig wlan1 essid DOBRA_VODA #Nastavení jména AP

iwconfig wlan1 txpower 10

#**********

#omezeni přístupu na AP podle MAC adres karet

iwpriv wlan1 maccmd 1

#povoleni klienti, kteří se mohou přihlásit na naše AP, filtrováni podle MAC adres.

příkaz iwpriv je součástí wireless tools a máme ho tedy nainstalován v /usr/local/sbin

iwpriv wlan1 addmac 00:60:B3:71:55:00

iwpriv wlan1 addmac 00:60:B3:73:3C:16

iwpriv wlan1 addmac 00:60:B3:71:54:CF

iwpriv wlan1 addmac 00:60:B3:6A:5D:A1

iwpriv wlan1 addmac 00:60:B3:6A:65:28

tímto máme nastaveno vše bezdrátové a je třeba nastavit IP protokol

ifconfig wlan0 10.23.80.23 netmask 255.255.255.0 # příkazem ifconfig se na Linuxu

#nastavují IP parametry na jednotlivá rozhraní Tento příkaz tedy nastavý IP adresu a masku #zařízení

ifconfig wlan1 192.168.1.254 netmask 255.255.255.0

ifconfig eth0 192.168.2.254 netmask 255.255.255.0 #Nastavení IP adresy ethernetové #kartě. V Linuxu jsou ethernetové karty pojmenovávány eth0 a opět inkrementálně dále dle #počtu ethernetových karet eth1, eth2 a tak dále.

route add default gateway 10.23.80.254 #Nastavení defaultní routy - gatewaye

echo 1 > /proc/sys/net/ipv4/ip_forward #Nastavení předávání paketů mezi rozhraními. Bez #tohoto nepředá jádro paket z jednoho rozhraní druhému a paket tedy neprojde počítačem.

iptables -t nat -A POSTROUTING -o wlan0 -j SNAT --to-source 10.23.80.23 #Nastavení #maškarády – NAT překladu adres. Opět by stálo za mnohem bližší vysvětlení, ale obávám #se že toto již je opravdu velice hodně nad rámec diplomové práce. Snad jen že si počítač – #router udržuje tabulku adres spojení inicializovaných z lokální sítě směrem ven a dle ní #rozděluje pak provoz přicházející z venkovní sítě jednotlivým počítačům v lokální síti. #Výhodou i nevýhodou tohoto řešení je, že počítače v lokální síti jsou odděleny od #venkovní sítě a z venkovní sítě se na ně nedá bez dalšího nastavení na routeru inicializovat #spojení . [13, 14]

3.7.6.3 - Konfigurace *bridge*

Toto je tedy kompletní výpis nastavení nastavení linuxového přístupového bodu se dvěma bezdrátovýma WiFi kartami Xi-626 a jedné ethernetové síťové karty firmy 3Com 3c590 v modu AP i klient. Dále bych rád ukázal, jaké další věci se dají dělat s Linuxem a podporovanými WiFi kartami. Vytvoříme si linuxový *bridge*. *Bridge* funguje tak, že se zařízení, v našem případě počítač s Linuxem, jednou ethernet kartou a jednou WiFi kartou, přepne do režimu ve kterém se chová jako síťový prvek, nejlépe přirovnatelný k *HUBu*. Chová se tak že, veškerý provoz z jednoho zařízení směruje do ostatních. V našem případě vše co přijde na ethernetový port se bez jakéhokoli zpracovávání dostane výstup z WiFi karty tedy na anténu a obráceně vše z bezdrátové karty se dostane bez zpracovávání do

ethernetové karty. Toto zařízení tedy samo nemusí mít vlastní IP adresu a funguje jako propojka, most, bridge mezi dvěma sítěmi, které takto spojí v jednu.

Nyní si ukážeme realizaci tohoto bridge pomocí Linuxu. Potřeba je pouze mít povolený bridge v jádře. Při kompilaci jádra volba Networking – Networking options – 802.1d Ethernet bridging a stažený balík ovládacích programů bridge-utils. (http://bridge.sourceforge.net/). Současná verze (prosinec 2005) je bridge-utils-1.0.6.

V Gentoo Linuxu nám stačí pouze zadat

root@Puda:~#emerge bridge-utils,

Vše se stáhne automaticky, přeloží a nainstaluje. Pakliže nedisponujeme kvalitní databází Gentoo linuxu – Portage, musíme vše zajistit ručně. Stáhneme tedy aktuální verzi bridge-utils a dále postupujeme klasickou linuxovou trojkombinací, ./configure, make, make install.

root@Puda:~#tar -xzvf bridge-utils-1.0.6.tar.gz

root@Puda:~#cd bridge-utils-1.0.6

root@Puda:~#./configure

root@Puda:~#make

root@Puda:~#make install

Bridge-utils jsou nainstalované.

Pokud děláme bridge, který se má pouštět při každém startu systému, je opět vhodné zařadit do startovacího skriptu /etc/rc.d/rc.local jeho spouštěcí příkazy. Skript bude vypadat tedy takto:

```
#!/bin/sh

#Každý bash skript musí začínat tímto #!/bin/sh. říká se tím bashi že se jedná o dávkový
#soubor, a že se má zpracovat interpretrem bash.

# /etc/rc.d/rc.local:  Local system initialization script.

#

# Put any local setup commands in here:

modprobe 3c59x
```

modprobe hostap_pci

modprobe hostap_crypt

iwconfig wlan0 channel 3 #nastevení karty na třetí kanál

iwconfig wlan0 mode managed

iwconfig essid STARNET_122

iwconfig wlan0 key 7855328572

#konfigurace bridge

brctl addbr br0 #Vytvoření virtuálního rozhraní bridge br0

brctl addif br0 eth0 #Přiřazení zařízení eth0 do bridge

brctl addif br0 wlan0 #Přiřazení zařízení wlan0 do bridge

A je to hotové. Ačkoliv bridge nepotřebuje IP adresu, je poměrně šikovné mu adresu přiřadit z důvodu dálkové správy. Adresa se potom přiřazuje virtuálnímu rozhraní tedy na konec souboru /etc/rc.d/rc.local přidáme ještě ifconfig br0 IP adresa. [13, 14]

3.7.6.4 - Další důležité parametry příkazu *iwconfig*

Dále si ukážeme které další důležité parametry se je možné nastavovat pomocí programu iwconfig. Nastavení některých parametrů může velice pomoci při ladění problémového spoje. Zde je výpis parametrů programu iwconfig. Některé nejdůležitější parametry již známe, ty jsme si ukázali v předchozích příkladech a proto se jim již nebudu věnovat a budu se věnovat parametrům ovlivňující kvalitu spoje.

root@Puda:~# iwconfig --help

Usage: iwconfig interface [essid {NNlonloff}]

[mode {managedlad-hocl...}

[freq N.NNNN[klMlG]]

[channel N]

[sens N]

[nick N]

[rate {N|auto|fixed}]

[rts {N|auto|fixed|off}]

[frag {N|auto|fixed|off}]

[enc {NNNN-NNNN|off}]

[power {period N|timeout N}]

[txpower N {mW|dBm}]

[commit]

Check man pages for more details.

Parametry freq a channel jsou totožné a nastavuje se jimi frekvence na jaké má karta pracovat. Již jsem se o tomto parametru zmiňoval v konfiguračním souboru. Zde je převodní tabulka mezi kanály a frekvencemi.
Kanály dle standardu IEEE 802.11b.

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

Tabulka 4: Převodní tabulka mezi kanálem a frekvencí.[5]

Dalším z parametrů o kterém si povíme je sens, z anglického slova sensitivity, česky citlivost. Citlivost přijímače se uvádí jako minimální napětí na anténní svorce přijímače, na které přijímač reaguje při stanoveném poměru signál/šum. Je-li citlivost přijímače např. 0,5 mV pro poměr signál/šum 10 dB, znamená to, že vlastní šum přijímače je 10 dB pod 0,5 mV. Někdy se citlivost uvádí také jako MDS (Minimum Discernible Signal) a bývá vyjádřen v dBm (výkonová úroveň vztažená k miliwattu, 0 dBm je 1 mW). Používá se především u přijímačů, u kterých se na výstupu uvažuje slyšitelný nf signál. MDS tedy vyjadřuje výkonovou úroveň, kterou je nutné přivést na anténní svorku přijímače, aby byl na výstupu patrný slyšitelný signál. Pojem „slyšitelný" bývá definován statisticky, signál musí slyšet definované procento osob, zúčastněných na testech. Ve VKV (Velmi Krátké Vlny) technice však bývá citlivost nejčastěji vyjadřována jako šumové číslo, udávající (v dB) kolikrát měřený přijímač šumí víc, než by za uvažované okolní teploty šuměl čistě ohmický odpor, rovný vstupní impedanci přijímače. Předpokládá se samozřejmě, že vstupní impedance přijímače je čistě reálná, což však málokdy bývá pravda. Pro naše úvahy o WiFi připojení však stačí si uvědomit, že šum neovlivníme, ať se jedná o šumové číslo přijímače nebo o průmyslový šum. Nyní již prakticky k nastavení citlivosti přijímače v operačním systému Linux.

root@Puda:~#iwconfig wlan0 sens 1

přičemž parametr sens může nabývat hodnot 1, 2, 3 kde 1 je největší citlivost a 3 nejmenší. Tento parametr se užívá v silně zarušeném prostředí, kde při snížení citlivosti přijímače se do zařízení dostane pouze silnější signál a slabé rušivé signály neruší přijímání požadovaného signálu.

Další parametr je rate (iwconfig wlan0 [rate {N|auto|fixed}]), což se dá přeložit do českého jazyka jako rychlost. Rychlost přenosu. Tato rychlost je rychlost kterou zařízení komunikuje s jinými bezdrátovými zařízeními. Možnosti jsou 1; 2; 5,5; 11 Mb/s. V režimu klient není nutné tuto rychlost nastavovat, jelikož si klient vyjedná nejvyšší možnou rychlost kterou může komunikovat s přípojným bodem a v průběhu spojení ji může měnit. To je volba „auto". Volba „fixed" naopak kartě říká, že se má držet na požadované rychlosti a neměnit ji. Používá se u *access pointů*, které mají pracovat na nižší než maximální rychlosti.

Parametr [rts {N|auto|fixed|off}] rts threshold (Request to send) udává minimální velikost fragmentu, při které nuceně vyšle handshake (jedná se o potvrzení že vysílací médium je volné), aby se ujistil, že médium je volné a je možno vysílat. Použije se pokud je v okolí větší množství klientů, a zajišťuje, aby nevysílali přes sebe. Obvyklé hodnoty

jsou 0 bytů ÷ 2347 bytů a čím vyšší, tím samozřejmě lepší, protože každý vynucený handshake zvyšuje režii protokolu a tím i zpomaluje přenos. Defaultní nastavení bývá na maximum a nastavuje se až v případě ladění špatně fungujícího spoje na klientech, na *access pointech* ne, protože ty komunikují s nastavením dle potřeb klientů. Volby jsou opět buď konkrétní číslo, nebo nastavování automaticky s možností že bude za běhu měněno dle potřeby, fixed – neměnné a vypnuto – off. V tomto případě se nastaví na maximum a handshake se provádí pouze při zahajování spojení.

Parametr [frag {N|auto|fixed|off}] - fragmentation threshold udává maximální velikost paketu na WiFi komunikační vrstvě - pokud je prostředí zarušené natolik, ze se nepodaří v pořádku odesílat cele IP pakety (tj. v kuse), díky fragmentation threshold se IP pakety rozdělí na menší, které - statisticky - mají větší šanci na projít zarušeným prosředím. Fragmentation threshold pak udává maximální velikost (v bytech) toho fragmentu. Hodnoty jsou od 256 do 2346 a čím většího paketu je možno dosáhnout, tím je spojení rychlejší. Problém ale nastává při ztrátách paketů. Při ztrátě velkého paketu protokol IP zajistí, že je paket vysílán znova, ale větší paket obsahuje samozřejmě více dat a v případě jejich ztráty a opětovného vysílání má přenos velké odezvy a na příklad pro IP telefonii je ztráta velkého paketu naprosto nevhodná. Malé pakety zase mají tu nevýhodu, že se zbytečně zvětšuje režie protokolu, protože se ke každému paketu přidává ještě hlavička IP a čím jsou pakety menší, tím je hlaviček více. Opět pokud je to možné je dobré tento parametr nenastavovat a nastavovat ho až v případě ladění hůře fungujícího spoje opět na klientovi.

Parametr [enc {NNNN-NNNN|off}] nebo [key {NNNN-NNNN|off}], jde o ten samý parametr a slouží k nastavení klíče pro šifrování WEP. Již jsme si ho popisovali v konfiguračním souboru. Lze jej zadat i v ASCII tvaru a sice takto:
iwconfig wlan0 key s:klíč.

Parametr [power {period N|timeout N}] se používá k manipulaci s energii šetřícími funkcemi PCI karty. Pomocí tohoto prarametru se karta uvádí do a z režimu spánku dle zadaných parametrů period či timeout.

Předposledním parametrem je [txpower N {mW|dBm}]. Toto je důležitý parametr a pomocí něj se nastavuje výstupní výkon WiFi karty. Jak jeho popis napovídá, hodnoty lze zadávat ve dvou formátech a sice v miliwattech a decibelech na metr. Tento parametr je důležitý právě pro dodržení limitu ČTU (dříve dle generální licence č. GL-12/R/2000, nyní dle všeobecného oprávnění č. VO – R/12/XX.2005 – viz v příloze 4), který říká že v bezlicenčním pásmu 2,4 GHz je maximální vyzářený výkon na anténě 100mW (20dBm) a

proto je třeba výkon zařízení spočítat a zkontrolovat. Zde si ukážeme pouze velmi zjednodušeně počítání ekvivalentního izotropicky vyzářeného výkonu – EIRP (Effective Isotropic Radiated Power).

EIRP = Vysílací výkon karty (zařízení) – útlum na kabelu a konektorech + zisk antény

Mějme tedy WiFi kartu XI-626, 5 metrů kabelu RG85 s útlumem 0,78 dBm, dva konektory, jeden reverzní SMA *Female* a jeden SMA *Male* s s útlumem obou 0,5dbm a sektorovou anténu se ziskem 7,5 dBi. Jaký nastavit vysílací výkon karty – x?

EIRP = x - 5*0,78 – 0,5 + 7,5

20 = x – 5*0,78 – 0,5 + 7,5

x = 20 + 5*0,78 + 0,5 – 7,5

x = 20 + 3,9 + 0,5 – 7,5

x = 24,4 – 7,5

x = 16,9 dBm

Na kartě tedy musíme nastavit menší výkon než 16,9 dBm abychom nepřekročili limity povolené ČTU, takže například:

root@Puda:~#iwconfig wlan0 txpower 16 dBm

nastaví požadovaný výstupní výkon karty celkový výkon tudíž nepřesáhne limit ČTU.

Ještě je potřeba ukázat převod mezi dB a miliwatty. Tedy zisk 10 mW je v decibelech 10*log(10)=10 dB. Zisk 100 mW je 10*log(100)=20 dB. Obdobně zisk 1000 mW je 30 dB atd. Útlum 0.1 mW je -10 dB, 0.01 mW je -20 dB atd. [3, 12]

Posledním parametrem je commit. Některé karty nemění svá nastavení okamžitě po jejich zadání programem iwconfig, těmto kartám je třeba říci, aby aktualizovaly nastavení a to se udělá právě pomocí parametru commit, přeloženo do češtiny to znamená proveď, čili proveď změny nastavení karty. [11]

Nyní máme probrány již všechny parametry programu iwconfig probrané a zbývá nám ukázat si ještě nějaké výhody, které nám umožňuje PCI karta zapojená v linuxovém počítači. První z nich je takzvané „scanování" okolí. Trochu jsem se o tomto zmínil při konfiguraci hardwarového *access pointu*, nyní si ukážeme možnosti linuxového *scanovacího* programu Kismet.

3.7.6.5 - Scanování ISM pásma pomocí programu Kismet

Kismet je opět volně ke stažení a se zdrojovými kódy pod licencí GPL na adrese http://www.kismetwireless.net/. Kismet detekuje sítě pasivním sbíráním paketů, dokáže

najít standardní přístupové body, utajené přístupové body i utajené sítě včetně IP a MAC adres.

Instalace v Gentoo Linuxu se provede opět velice jednoduše

root@Puda:~#emerge kismet

v jiných linuxových distribucích se stáhnou zdrojové kódy z http://www.kismetwireless.net/download.shtml, rozpakují

root@Puda:~#tar -xzvf kismet-2005-08-R1.tar.gz

přepneme se do adresáře s kismetem, a známou linuxovou trojkombinací

root@Puda:~#./configure

root@Puda:~#make

root@Puda:~#make install

přeložíme a nainstalujeme. Kismet se skládá ze dvou částí. Serverové části a klienta. Při spouštění nejprve spustíme kismet_monitor, který přepne kartu do monitorovacího módu. Další krokem je spuštění kismet serveru, který se provede spuštěním kismet_server a karta již scanuje a výsledky ukládá na disk, přednastavený adresář kam se soubory ukládají je /home/uzivatel/.kismet/ do několika souborů. Nejdůležitější soubory jsou Kismet-Aug-15-2005-1.csv, který obsahuje seznam nascanovaných počítačů se všemi zjištěnými parametry oddělený středníky , takže je možné jej dále strojově zpracovávat či data importovat například do MS Excelu a pracovat s nimi tam. Výpis souboru je v příloze 2. Další soubor je Kismet-Aug-15-2005-1.dump, obsahující veškerá data, která program nascanoval pro pozdější analýzu. Tento soubor může po delším scanování zabírat i stovky megabytů na harddisku.A poslední důležitý soubor je Kismet-Aug-15-2005-1.network obsahující data o jednotlivých sítích. Soubor je možné si prohlédnout v příloze 3.

4. Bezpečnost v bezdrátových sítích

Nyní si probereme problematiku zabezpečení bezdrátových sítí.

4.1 - WEP (Wired Equivalent Privacy)

Zajišťuje šifrování rámců na 2. síťové vrstvě. Šifruje tedy veškeré rámce (blok binárních dat), které vedou od klienta k AP a ne pouze určité služby. Pokud je však AP připojen do Internetu, tak mezi AP a internetovým serverem šifrování neprobíhá. Právě

použitá šifra je u WEP-u největší problém.

K šifrovaní se používá algoritmus RC4, jehož autorem je R. Rivest a zveřejněn byl v roce 1994. Algoritmus používá proudovou symetrickou šifru s délkou klíče 40, 104 a 232 bitů. Již v roce 2001 však bylo v algoritmu objeveno hned několik bezpečnostních nedostatků. Se symetrickým šifrováním je problém v tom, že někde musí mít klient uložený statický klíč, kterým šifruje a zároveň dešifruje komunikaci. Lepší výrobci chrání přístup ke klíči ve speciální paměti síťové karty (NVRAM), ke které lze přistupovat jen pod heslem. Bohužel tímto způsobem to zdaleka nedělají všichni a najdou se i případy, kdy je klíč uložen v registrech a to v otevřené podobě.

Proudová šifra generuje pseudonáhodný *stream* o stejné délce jakou má zpráva, tzn. délka klíče podle potřeby mění velikost. Generátor pseudonáhodných čísel, který podle pravidel rozšíří délku klíče se nazývá PRNG. Šifrování probíhá jednoduchou operací XOR mezi zprávou a klíčovým *streamem* a dešifrování probíhá reverzně. WEP bohužel nijak neřeší distribuci klíče a tak je musíme ve většině případů manuálně zapsat do konfigurace zařízení. Tím trochu odpadá podstata šifrování. Útočník sice zatím klíč nezná, ale oprávněný uživatel ano a tak pro něj není složité komunikaci dešifrovat a protože 70% útoků je vedeno zevnitř sítě, tak tento fakt považuji za velký bezpečnostní nedostatek. Ani oprávněný uživatel by o podobě klíče neměl vůbec vědět.

Odesílatel i příjemce musí mít stejný klíč používaný k šifrování/dešifrování komunikace. Pro vyšší bezpečnost je nutné klíč průběžně obměňovat. To ale WEP ani RC4 nijak neřeší a tak jediný možný způsob změny klíče je opětovné nahrazení stávajícího v konfiguraci adaptéru. U distribuce klíčů je problém, protože případný útočník může nový klíč při předání získat. Proto to v dnešních sítích chráněných WEP-em vypadá tak, že se jeden rok používá stejný klíč. Přičemž v lepších případech by se měl klíč měnit po několika minutách. Proč tedy právě tato šifra ? Jednoduše proto, že ji lze snadno implementovat do hardwaru bezdrátových adaptérů a díky tomu nemá aktivování šifrování téměř žádný vliv na výkon počítače.

Zašifrování stejné zprávy symetrickou šifrou totiž pokaždé generuje stejnou šifrovanou zprávu a tím pádem je mnohem jednoduší klíč uhodnout. Proto je součástí WEP ještě inicializační vektor (IV), který se mění s každým paketem a doplňuje klíč o dalších 24 bitů. Při použití WEP-u s klíčem dlouhým 128 bitů má klíč pouze 104 bitů + 24 bitů IV. Generování IV zajišťuje vysílací strana, která ho nejenom použije k sestavení šifrovaného streamu, ale přidá ho v otevřené podobě i do záhlaví rámce. Tím by se mohlo zdát, že se

pokaždé použije "jiný klíč" a šifra je tím bezpečnější, ale není tomu tak. Unikátních IV je pouze 224 a pokud se tedy odešle 224 paketů, začne se IV opakovat. Inicializačním vektorem se tedy nic nevyřeší a šifra je stále napadnutelná řadou útoků. Navíc prodloužení klíče má k délce jeho luštění lineární závislost => pro 2x delší klíč je potřeba pouze 2x více času k dešifrování.

Integritu šifrované zprávy zajišťuje známá funkce CRC-32 (Cyclic Redundancy Check), jejíž hodnota je společně s daty zašifrovaná v těle zprávy. Bohužel však díky lineárnosti funkce CRC32 ji lze obelstít určitou formou záměny bitů, které nedokáže odhalit.[15]

4.2 - WPA (WiFi Protected Access)

WPA je novější bezpečnostní mechanizmus a původně měl opravit chyby, kterých se WiFi Aliance dopustila u WEP-u. Sice nešťastně používá stejný šifrovací algoritmus RC4, kvůli jednoduchému upgradu firmwaru stávajících zařízení, ale určitě sebou přináší řadu vylepšení. Standardně používá 128 bitový dynamický klíč, který se mění každých 10 000 paketů. Dalším zlepšením je MIC (Message Integrity Check), jež je používán současně s CRC32 a tím řeší jeho nedostatky, díky kterým bylo možné změnit zprávu při zachování stejného kontrolního součtu. Nyní přejdu dále k popisu metod útoků.[15]

4.3 - Bezpečnostní nedostatky

Programátoři Scott Fluhrer, Itsik Mantin a Adi Shamir publikovali zprávu ! "Weakness in the Key Scheduling Algorithm of RC4" (slabina v algoritmu plánování klíčů RC4), která popisuje metodu (FMS – Fluhrer-Mantin-Shamir dle jmen autorů) umožňující prolomit řídící WEP klíč. Prvním programem, který dokázal pasivním odposloucháváním komunikace derivovat šifrovací klíč byl AirSnort (http://airsnort.shmoo.com). AirSnort byl uveřejněn o víkendu 17. srpna 2001 i se zdrojovými kódy a tehdy poprvé se začalo o slabé bezpečnosti WiFi sítí mluvit v širším měřítku. Autoři programu (Jeremy Bruestle a Blake Hegerle) uvádějí, že jim sestavení programu trvalo zhruba 24 hodin. AirSnort využíval metodu FMS, jejíž podmínkou bylo odposlechnutí obrovského množství paketů. Dalším problémem bylo, že klíč lze *cracknout* jen za pomocí "slabých" paketů s unikátním inicializačním vektorem (IV), takže v prvopočátcích byl AirSnort účinný až po značném úsílí. Dnes již ale existují mnohem efektivnější a promyšlenější metody a nástroje sloužící

k derivace klíče, jako např. Aircrack (http://www.cr0.net:8040/code/network/) a WepLab (http://weplab.sourceforge.net/). Tuto "novou éru" *crackování* odstartoval dne 8. srpna 2004 hacker s přezdívkou KoreK se svojí novou metodou statistické kryptoanalýzy, která se zhmotnila v nástroji chopper. Tato metoda změnila celou podstatu útoku FMS a již nebylo zapotřebí slabých paketů. Základní složkou útoku je zachycení velkého množství paketů se stejným inicializačním vektorem. Útok je často možný po odposlechnutí řádově statisíců paketů. Tato metoda byla samozřejmě poupravena a portována do programů aircrack a WepLab. Teď konečně přejdeme k jednotlivým scénářům útoku, kde se budu snažit uvést jak slabiny protokolů samotných, tak i modely špatné konfigurace přístupového bodu (AP).[15]

4.3.1 - Podvržení MAC adresy

Pokud není AP úplně nezabezpečený, tak filtrování MAC adres bývá první překážka, kterou ale lze obejít během několika sekund. Teď nebudeme uvažovat o šifrovaném AP, ale o takovém, který pouze podle MAC adres povoluje přístup a tím řeší autentizaci. My jednoduše odposlechneme jednu z používaných adres a přiřadíme ji své WiFi kartě. Pod Windows lze MAC adresu změnit programem SMAC nebo v registrech Windows pomocí nástroje regedit upravit tento záznam: HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/Class/4936E972-xxxx-xxxx.

Pod Linuxem jednoduše za použití nástroje ifconfig:

root@Puda:~# ifconfig eth0 down

root@Puda:~# ifconfig eth0 hw ether 00:00:00:00:00:00

root@Puda:~# ifconfig eth0 up

Problém s tímto útokem je ten, že proti němu neexistuje žádná inteligentní obrana a útočník může zcela vyřadit regulérního klienta a proto je lepší tuto ochranu ani nepoužívat a přístup řešit na vyšší vrstvě IP protokolu.[15]

4.3.2 - Podvržení přístupového bodu

Představme si situaci, kdy se klient přihlašuje do sítě přes šifrované stránky uložené na AP. Útočník nakonfiguruje na počítači s Linuxem a WiFi kartou *access point*, okopíruje design a formu stránek na kterých se uživatelé autentizují, spustí *webserver* Apache a ke

kartě připojí silnou anténu. Anténa vysílající na stejném kanále a se stejným SSID, jako pravý AP, musí mít vyšší zisk a tím se uživatel, místo na pravé AP, připojí na počítač útočníka. Otevře se mu stránka, kam zadá login a heslo, které útočník uloží do databáze a má vše potřebné k regulérnímu přihlášení.

Další možností je že útočník nabídne uživateli přesně to co chce. Tím myslím překryje signálem pravé AP, nechá klienta se připojit a povolí mu jen port 80 pro surfování na internetu. Povolí pouze port 80, ale ne port 443, který se používá k zabezpečenému přístupu na webové stránky pomocí SSL (Secure Socket Layer). Takže uživatel si bude číst emaily, nakupovat kreditní kartou v eshopu atp. a útočník v roli prostředníka mezitím může odposlechnout veškeré soukromé informace.

Opět shrnutí na závěr. Obrana WiFi sítí je složitý problém který se řeší pomocí VPN (Virtual Private Network), ssh (secure shell) tunely či šifrování pomocí IPsec. Všechny tyto způsoby zabrání útočníkovy odposlechnout data pomocí *Man In The Middle* (typický útok v sítích s *HUBy*) útoku i se pomocí tohoto dá řešit problém autorizace. Stinná stránka ale je, že pro šifrování více spojení je potřeba silnější hardware, protože veškeré šifrování provádí přímo procesor a ne např. WiFi karta jak je tomu u šifrování pomocí WEP.

5. Závěr

Závěrem bych dodal, že ač je WiFi již poměrně hodně rozšířené, materiály, a hlavně materiály v češtině, se shánějí velice těžko. Vycházel jsem proto hlavně z anglicky psané literatury, internetových diskusí a z praktických zkušeností získaných v zaměstnání. Z těchto pramenů a v souladu s cíli práce, jsem vytvořil text který by čtenáři měl být nápomocen při orientaci v problematice WiFi sítí, při volbě technologie pro vytvoření počítačové sítě či datové trasy, ale hlavně praktický průvodce pro vytvoření WiFi sítě. V práci jsem se hodně věnoval nastavování WiFi v operačním systému GNU Linux a kdyby práce umožňovala větší rozsah, věnoval bych se zřejmě mnohem podrobněji konfiguraci linuxového routeru. Podrobněji bych popsal jaderný linuxový *firewall* iptables, který je od řady 2.4 v linuxovém jádře obsažený, ukázal bych značkování paketů pro nastavování QoS, *shapingu*, pro počítání dat a pro nastavení FUP (Fair User Policy). Také bych se mnohem hlouběji ponořil do problematiky bezpečnosti WiFi i ethernetových sítí. Jelikož jsem ale psal pouze o části bezdrátových přenosů a sice o technologii WiFi, nebylo by to zcela k tématu.

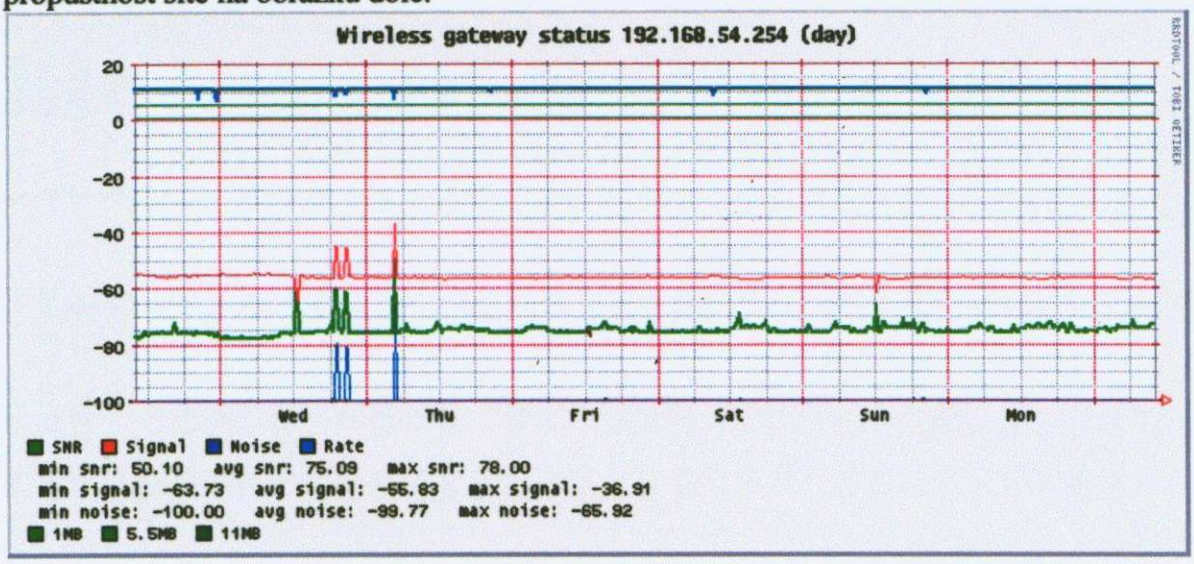
Seznam použité literatury:

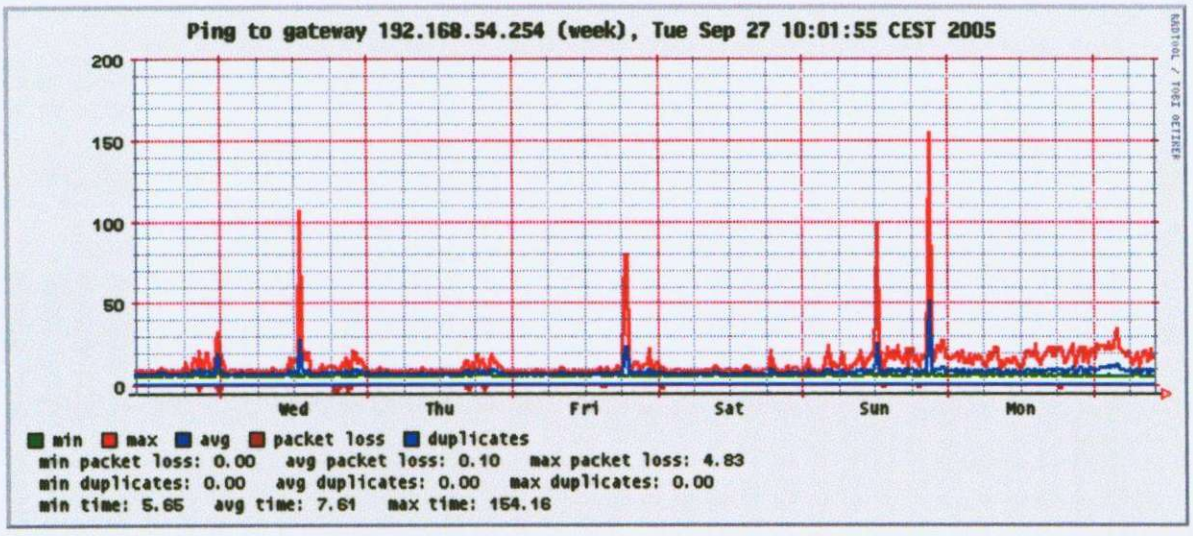
[1] ROSS, JOHN: The Book of Wi-Fi, No Starch Press, 2003.
[2] http://standards.ieee.org/getieee802/download/802.11-1999.pdf
[3] ZANDL, PATRIK: Bezdrátové sítě WiFi Praktický průvodce, Computer Press, 2003.
[4] DUNTEMANN, JEFF: Wi-Fi Guide, Oreilly & Associates Inc., 2004.
[5] HAROLD, DAVIS – MANSFIELD, RICHARD: The Wi-Fi Experience Everyone`s Guide to 802.11b Wireless networking, Que, 2002.
[6] http://grouper.ieee.org/groups/802/11/
[7] http://en.wikipedia.org/wiki/IEEE_802.11
[8] PROCHÁZKA, M: Antény: encyklopedická příručka, BEN - technická literatura, 2002.
[9] Firemní materiály D-Link®, Katalog produktů, 2005.
[10] Firemní materiály D-Link®, Manuál AWL-900AP+, 2005.
[11] Manuálové stránky programu iwconfig(8).
[12] http://www.ctu.cz/1/download/Navrhy/VO_R_12_XX.2005.doc, příloha 6.
[13] NEMETH, EVI - SNYDER, GARTH - HEIN,T,R: Linux - Kompletní příručka administrátora, Computer Press, 2004.
[14] Kolektiv autorů: Linux Dokumentační projekt, 3. aktualizované vydání, Computer Press, 2003.
[15] SCAMBRAY, J - MCCLURE, S - KURTZ, G: Hacking bez tajemství, 3. aktualizované vydání, Computer Press, 2004.

Seznam příloh

Příloha č. 1 – Grafy parametrů přenosu

Na grafu je vidět nepatrné zhoršení podmínek pro bezdrátový přenos vlivem prudkého deště mezi středou a čtvrtkem, který ale nemá téměř vliv na výslednou propustnost sítě na obrázku dole.





Příloha č. 2 - Kismet csv soubor

Network	NetType	ESSID	BSSID	Info	Channel	Maxrate	WEP	LLC	Data	Crypt	Weak	Total	BestQualit	BestSignal
1	infrastructu	CZFreeCB_Me	00:4F:62:03:9C:E	None	4	0.0	No	1174	4171	0	0	5345	0	31
2	infrastructu	STARNET_13	00:50:FC:D7:05:[	None	3	0.0	Yes	1583	5116	5116	0	6699	0	31
3	infrastructu	STARNET_122	00:03:2F:19:21:8	None	7	0.0	Yes	356	17597	17597	1	17953	0	49
4	infrastructu	CZFreeCB_Suc	00:60:B3:65:6C:E	None	6	11.0	No	1118	6	0	0	1124	0	32
5	infrastructu	<no ssid>	00:30:4F:3D:D6:(	None	6	11.0	Yes	1307	0	0	0	1307	0	33
6	infrastructu	STARNET_231	00:03:2F:1D:8A:5	None	9	0.0	Yes	799	2143	2143	0	2942	0	29
7	infrastructu	STARNET_11	00:03:2F:17:BF:1	None	8	11.0	Yes	1199	1918	1918	0	3117	0	25
8	infrastructu	SV_SV1	00:11:D8:60:4D:7	None	9	54.0	No	70	15	0	0	85	0	10
9	infrastructu	<no ssid>	00:60:B3:8C:8E:9	None	0	0.0	No	0	2781	0	0	2781	0	23
10	infrastructu	<no ssid>	00:60:1D:23:4F:7	None	7	11.0	No	319	117	0	0	436	0	20
11	infrastructu	STARNET_23	00:03:2F:18:0D:4	None	9	11.0	Yes	411	780	780	0	1191	0	19
12	infrastructu	<no ssid>	00:40:96:56:CC:A	POHODA_	10	11.0	No	1529	2128	0	0	3657	0	33
13	infrastructu	CZFreeCB_Kal	00:E0:98:BE:8C:2	None	11	11.0	No	634	22	0	0	656	0	20
14	infrastructu	CZFreeCB_Hef	00:4F:62:03:A8:2	None	10	0.0	No	291	1370	0	0	1661	0	18
15	infrastructu	perex.cz|Mokre	00:4F:62:01:FB:6	None	1	5.V	Yes	272	0	0	0	272	0	21
16	infrastructu	POH_NET6	00:40:96:33:B6:A	POHODA_	1	11.0	No	886	4931	0	0	5817	0	25
17	infrastructu	<no ssid>	00:40:96:37:17:2I	VAK_CB	1	11.0	No	305	0	0	0	305	0	13
18	infrastructu	CZFreeCB_Me	00:02:B3:94:07:D	None	1	11.0	No	143	5	0	0	148	0	11
19	infrastructu	TSNET.CB_Vrb	00:60:B3:65:AF:E	None	1	11.0	Yes	305	2	2	0	307	0	20
20	infrastructu	DomaB	00:E0:98:4E:17:6	None	1	11.0	Yes	223	0	0	0	223	0	11
21	infrastructu	STARNET_121	00:03:2F:17:BD:4	None	3	11.0	Yes	543	791	791	0	1334	0	44
22	infrastructu	DORA	00:00:AA:BB:CC:	None	1	11.0	No	79	0	0	0	79	0	12
23	infrastructu	DDDV-B-P	00:0F:3D:AF:D5:!	None	6	36.0	No	20	5	0	0	25	0	12
24	infrastructu	CZFreeCB_Lidi	00:60:B3:6E:1D:[	None	6	11.0	No	20	1	0	0	21	0	11
25	probe	STARNET_13	00:E0:98:BE:D5:(	None	0	1.0	No	2	0	0	0	2	0	9
26	infrastructu	SPS-CB	00:0D:88:82:CE:3	None	6	22.0	No	31	0	0	0	31	0	11
27	infrastructu	STARNET_221	00:4F:62:00:06:3	None	6	0.0	Yes	52	43	43	0	95	0	16
28	infrastructu	HOME	00:90:4B:87:B3:F	None	6	11.0	Yes	97	0	0	0	97	0	18
29	infrastructu	<no ssid>	00:E0:98:BE:A5:(	None	0	0.0	No	0	254	254	0	254	0	16
30	infrastructu	CZFreeCB_Ner	00:4F:62:03:8E:A	None	13	11.0	No	90	0	0	0	90	0	15
31	infrastructu	CAPE2_S12	00:60:B3:19:C4:9	None	2	11.0	No	73	27	0	0	100	0	10
32	infrastructu	cbmacd5821	00:04:DB:00:DB:4	None	2	11.0	Yes	72	0	0	0	72	0	9
33	infrastructu	perex.cz|Sindlo	00:11:D8:10:E2:3	None	7	11.0	Yes	121	11	11	0	132	0	16
34	infrastructu	STARNET_92	00:0E:8E:7A:36:8	None	3	11.0	Yes	133	4	4	0	137	0	16

35	infrastructu	SUCHAC	00:0D:54:F7:84:F	None	10	11.0	No	230	140	0	0	370	0	27
36	infrastructu	STARNET_22	00:03:2F:19:21:6	None	8	11.0	Yes	113	116	116	0	229	0	13
37	infrastructu	<no ssid>	00:40:96:44:2A:D	None	0	0.0	No	0	7	7	0	7	0	12
38	infrastructu	STARNET_61	00:03:2F:10:F7:F	None	4	0.0	Yes	3	96	96	0	99	0	15
39	infrastructu	STARNET_131	00:03:2F:1B:11:8	None	5	11.0	Yes	137	9	9	0	146	0	19
40	infrastructu	<no ssid>	00:D0:41:82:50:0	None	9	54.0	Yes	55	0	0	0	55	0	10
41	infrastructu	<no ssid>	00:80:48:36:53:2	None	0	0.0	No	0	3802	0	0	3802	0	37
42	infrastructu	CAPE1_S1	00:60:B3:19:FF:[	None	5	0.0	Yes	34	13	13	0	47	0	13
43	infrastructu	STARNET_201	00:E0:98:C5:94:[	None	5	11.0	Yes	62	37	37	0	99	0	14
44	infrastructu	STARNET_91	00:03:2F:17:B8:7	None	5	11.0	Yes	97	32	32	0	129	0	16
45	infrastructu	STARNET_173	00:4F:62:00:00:F	None	10	11.0	Yes	134	58	58	0	192	0	28
46	infrastructu	<no ssid>	00:11:09:0F:14:3	None	6	54.0	Yes	35	0	0	0	35	0	11
47	infrastructu	<no ssid>	00:40:96:25:7A:F	TEPLARN/	7	0.0	No	74	27	1	0	101	0	14
48	infrastructu	<no ssid>	00:40:96:48:94:7	1CB03-B1	4	11.0	Yes	97	22	22	0	119	0	29
49	infrastructu	STARNET_51	00:03:2F:0F:38:B	None	4	11.0	Yes	15	1	1	0	16	0	9
50	infrastructu	STARNET_14	00:03:2F:1B:11:C	None	7	0.0	Yes	11	15	15	0	26	0	22
51	infrastructu	STARNET_41	00:E0:98:BE:B4:	None	4	11.0	Yes	6	0	0	0	6	0	5
52	infrastructu	STARNET_01	00:E0:98:BE:A5:(	None	5	11.0	Yes	76	37	37	0	113	0	14
53	infrastructu	RedStar	00:09:5B:74:C5:1	None	10	11.0	No	3	0	0	0	3	0	6
54	infrastructu	perex.cz|Mokre_	00:11:2F:6B:D7:E	None	1	11.0	Yes	67	0	0	0	67	0	5
55	infrastructu	Doma	00:E0:98:4D:40:8	None	1	11.0	Yes	4	0	0	0	4	0	3
56	infrastructu	<no ssid>	00:11:D8:74:C7:4	None	0	0.0	No	0	8	8	0	8	0	9
57	infrastructu	STARNET_211	00:03:2F:1D:81:C	None	6	36.0	Yes	5	0	0	0	5	0	6
58	infrastructu	<no ssid>	00:03:2F:19:1A:E	None	0	0.0	No	0	1	0	0	1	0	9
59	infrastructu	Rosenet	00:E0:98:BE:D5:(	None	9	11.0	Yes	20	0	0	0	20	0	8
60	infrastructu	Kostka-Pohurka	00:40:F4:A9:F5:A	None	6	11.0	Yes	2	0	0	0	2	0	4
61	probe	POHODA_NET	00:09:B7:41:3D:1	None	0	11.0	No	8	0	0	0	8	0	12
62	infrastructu	Mikes	00:E0:98:4D:40:6	None	1	11.0	No	3	0	0	0	3	0	2
63	infrastructu	DBS_2	00:4F:62:03:AB:6	None	6	1.0	Yes	10	1	1	0	11	0	9
64	infrastructu	<no ssid>	00:60:B3:6E:1D:7	None	0	0.0	No	0	4	0	0	4	0	9
65	infrastructu	<no ssid>	00:E0:98:C5:92:[	None	0	0.0	No	0	11	0	0	11	0	13
66	infrastructu	perex.cz|Mokre_	00:11:D8:97:DF:(	None	1	11.0	Yes	25	0	0	0	25	0	11
67	infrastructu	STARNET_111	00:50:FC:D4:C3:I	None	11	11.0	Yes	11	0	0	0	11	0	11
68	infrastructu	<no ssid>	00:11:95:51:20:F	None	0	0.0	No	0	64	64	0	64	0	16
69	infrastructu	internet	00:02:2D:B7:20:7	None	3	11.0	No	3	0	0	0	3	0	10
70	infrastructu	<no ssid>	00:03:2F:17:BC:3	None	0	0.0	No	0	22	22	0	22	0	8

Příloha č. 3 - „Kismet networks" - zkráceno

```
Network 1: "CZFreeCB_Mephisto" BSSID: "00:4F:62:03:9C:EF"
    Type     : infrastructure
    Carrier  : 802.11b
    Info     : "None"
    Channel  : 04
    WEP      : "No"
    Maxrate  : 0.0
    LLC      : 1174
    Data     : 4171
    Crypt    : 0
    Weak     : 0
    Total    : 5345
    First    : "Mon Aug 15 17:05:55 2005"
    Last     : "Mon Aug 15 17:18:14 2005"
    Address found via TCP 10.108.0.0

Network 2: "STARNET_13" BSSID: "00:50:FC:D7:05:D6"
    Type     : infrastructure
    Carrier  : 802.11b
    Info     : "None"
    Channel  : 03
    WEP      : "Yes"
    Maxrate  : 0.0
    LLC      : 1583
    Data     : 5116
    Crypt    : 5116
    Weak     : 0
    Total    : 6699
    First    : "Mon Aug 15 17:05:55 2005"
    Last     : "Mon Aug 15 17:18:13 2005"

Network 3: "STARNET_122" BSSID: "00:03:2F:19:21:8F"
    Type     : infrastructure
    Carrier  : 802.11b
    Info     : "None"
    Channel  : 07
    WEP      : "Yes"
    Maxrate  : 0.0
    LLC      : 356
    Data     : 17597
    Crypt    : 17597
    Weak     : 1
    Total    : 17953
    First    : "Mon Aug 15 17:05:55 2005"
    Last     : "Mon Aug 15 17:18:14 2005"

Network 4: "CZFreeCB_SucheVrbne1a" BSSID: "00:60:B3:65:6C:E1"
    Type     : infrastructure
    Carrier  : 802.11b
    Info     : "None"
    Channel  : 06
    WEP      : "No"
    Maxrate  : 11.0
    LLC      : 1118
    Data     : 6
    Crypt    : 0
    Weak     : 0
    Total    : 1124
    First    : "Mon Aug 15 17:05:55 2005"
    Last     : "Mon Aug 15 17:18:14 2005"

Network 5: "<no ssid>" BSSID: "00:30:4F:3D:D6:61"
    Type     : infrastructure
    Carrier  : 802.11b
    Info     : "None"
    Channel  : 06
    WEP      : "Yes"
    Maxrate  : 11.0
    LLC      : 1307
    Data     : 0
    Crypt    : 0
    Weak     : 0
```

```
    Total    : 1307
    First    : "Mon Aug 15 17:05:55 2005"
    Last     : "Mon Aug 15 17:18:14 2005"

Network 6: "STARNET_231" BSSID: "00:03:2F:1D:8A:58"
    Type     : infrastructure
    Carrier  : 802.11b
    Info     : "None"
    Channel  : 09
    WEP      : "Yes"
    Maxrate  : 0.0
    LLC      : 799
    Data     : 2143
    Crypt    : 2143
    Weak     : 0
    Total    : 2942
    First    : "Mon Aug 15 17:05:55 2005"
    Last     : "Mon Aug 15 17:18:15 2005"

Network 7: "STARNET_11" BSSID: "00:03:2F:17:BF:1A"
    Type     : infrastructure
    Carrier  : 802.11b
    Info     : "None"
    Channel  : 08
    WEP      : "Yes"
    Maxrate  : 11.0
    LLC      : 1199
    Data     : 1918
    Crypt    : 1918
    Weak     : 0
    Total    : 3117
    First    : "Mon Aug 15 17:05:55 2005"
    Last     : "Mon Aug 15 17:18:14 2005"

Network 8: "SV_SV1" BSSID: "00:11:D8:60:4D:7B"
    Type     : infrastructure
    Carrier  : 802.11b
    Info     : "None"
    Channel  : 09
    WEP      : "No"
    Maxrate  : 54.0
    LLC      : 70
    Data     : 15
    Crypt    : 0
    Weak     : 0
    Total    : 85
    First    : "Mon Aug 15 17:05:55 2005"
    Last     : "Mon Aug 15 17:17:58 2005"
    Address found via TCP 10.108.1.163

Network 9: "<no ssid>" BSSID: "00:60:B3:8C:8E:97"
    Type     : infrastructure
    Carrier  : 802.11b
    Info     : "None"
    Channel  : 00
    WEP      : "No"
    Maxrate  : 0.0
    LLC      : 0
    Data     : 2781
    Crypt    : 0
    Weak     : 0
    Total    : 2781
    First    : "Mon Aug 15 17:05:55 2005"
    Last     : "Mon Aug 15 17:18:14 2005"
    Address found via TCP 192.168.100.253

Network 10: "<no ssid>" BSSID: "00:60:1D:23:4F:7E"
    Type     : infrastructure
    Carrier  : 802.11b
    Info     : "None"
    Channel  : 07
    WEP      : "No"
    Maxrate  : 11.0
    LLC      : 319
```

```
    Data      : 117
    Crypt     : 0
    Weak      : 0
    Total     : 436
    First     : "Mon Aug 15 17:05:55 2005"
    Last      : "Mon Aug 15 17:18:13 2005"
    Address found via ARP 195.47.121.93

Network 11: "STARNET_23" BSSID: "00:03:2F:18:0D:49"
    Type      : infrastructure
    Carrier   : 802.11b
    Info      : "None"
    Channel   : 09
    WEP       : "Yes"
    Maxrate   : 11.0
    LLC       : 411
    Data      : 780
    Crypt     : 780
    Weak      : 0
    Total     : 1191
    First     : "Mon Aug 15 17:05:55 2005"
    Last      : "Mon Aug 15 17:18:10 2005"

Network 12: "DORA" BSSID: "00:00:AA:BB:CC:0D"
    Type      : infrastructure
    Carrier   : 802.11b
    Info      : "None"
    Channel   : 01
    WEP       : "No"
    Maxrate   : 11.0
    LLC       : 79
    Data      : 0
    Crypt     : 0
    Weak      : 0
    Total     : 79
    First     : "Mon Aug 15 17:05:56 2005"
    Last      : "Mon Aug 15 17:18:13 2005"

Network 13: "STARNET_121" BSSID: "00:03:2F:17:BD:44"
    Type      : infrastructure
    Carrier   : 802.11b
    Info      : "None"
    Channel   : 03
    WEP       : "Yes"
    Maxrate   : 11.0
    LLC       : 543
    Data      : 791
    Crypt     : 791
    Weak      : 0
    Total     : 1334
    First     : "Mon Aug 15 17:05:56 2005"
    Last      : "Mon Aug 15 17:18:08 2005"

Network 14: "DomaB" BSSID: "00:E0:98:4E:17:64"
    Type      : infrastructure
    Carrier   : 802.11b
    Info      : "None"
    Channel   : 01
    WEP       : "Yes"
    Maxrate   : 11.0
    LLC       : 223
    Data      : 0
    Crypt     : 0
    Weak      : 0
    Total     : 223
    First     : "Mon Aug 15 17:05:56 2005"
    Last      : "Mon Aug 15 17:18:02 2005"

Network 15: "TSNET.CB_Vrbne" BSSID: "00:60:B3:65:AF:E9"
    Type      : infrastructure
    Carrier   : 802.11b
    Info      : "None"
    Channel   : 01
    WEP       : "Yes"
```

Příloha č. 4 – „http://www.ctu.cz/download/Navrhy/VO_R_12_XX.2005.doc“

Český telekomunikační úřad
se sídlem Sokolovská 219, Praha 9

Praha 23. května 2005
Č.j.: 23820/2005-613

N Á V R H

Český telekomunikační úřad (dále jen „Úřad“) jako věcně příslušný orgán státní správy podle § 108 odst. 1 písm. b) zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích) (dále jen „zákon“), a na základě výsledků veřejné konzultace uskutečněné podle § 130 a k provedení § 9 odst. 2 zákona jako opatření obecné povahy vydává

všeobecné oprávnění č. VO – R/12/XX.2005

k využívání rádiových kmitočtů a k provozování zařízení pro širokopásmový přenos dat na principu rozprostřeného spektra nebo OFDM v pásmech 2,4 GHz a 5 GHz.

Článek 1
Úvodní ustanovení

Všeobecné oprávnění stanoví podmínky pro využívání rádiových kmitočtů a provozování vysílacích rádiových zařízení pro širokopásmový přenos dat na principu rozprostřeného spektra nebo OFDM [1]) v pásmech 2,4 GHz a 5 GHz (dále jen „stanice“) fyzickými nebo právnickými osobami (dále jen „uživatel“) bez jakéhokoliv dalšího řízení u Úřadu.

Článek 2
Podmínky

(1) Všeobecné oprávnění platí na území České republiky.

(2) Stanice pracují v těchto kmitočtových pásmech a s těmito technickými parametry:

ozn.	kmitočtové pásmo	max. výkon	další podmínky

[1]) OFDM – ortogonální modulace s vícenásobným frekvenčním dělením (Orthogonal Frequency Division Multiplex).

a	2400,0 – 2483,5 MHz	100 mW e.i.r.p.	
b	5150–5250 MHz	200 mW střední e.i.r.p. [2])	pouze pro použití uvnitř jedné budovy
c	5250–5350 MHz	200 mW střední e.i.r.p. [2])	pouze pro použití uvnitř jedné budovy
d	5470–5725 MHz	1 W střední e.i.r.p. [2])	maximální střední spektrální hustota e.i.r.p. je 50 mW/MHz v libovolném 1 MHz úseku

(3) U systémů s rozprostřeným spektrem využívajících techniku přímé sekvence nebo modulaci OFDM v pásmu *a* nesmí spektrální hustota e.i.r.p. překročit hodnotu –20 dBW/1 MHz. Pro systémy s rozprostřeným spektrem, které využívají techniky přeskoku kmitočtu, nesmí spektrální hustota e.i.r.p. překročit hodnotu – 10 dBW/100 kHz.

(4) V pásmech *b* až *d* je maximální střední spektrální hustota e.i.r.p. omezena takto: v pásmu *b* (5150–5250 MHz) na 0,25 mW/25 kHz v libovolném 25 kHz úseku; v pásmu *c* (5250–5350 MHz) na 10 mW/MHz v libovolném 1 MHz úseku; v pásmu *d* (5470–5725 MHz) na 50 mW/MHz v libovolném 1 MHz úseku.

(5) Maximální vyzářený výkon e.i.r.p. a maximální střední spektrální hustota musí být dodrženy při libovolné kombinaci výstupního výkonu vysílače a použité antény.

(6) Stanice mohou být vybaveny pouze vestavěnou anténou nebo druhem / typem antény, který stanoví výrobce v návodu k obsluze. Stanice nesmějí být provozovány s přídavnými zesilovači vysokofrekvenčního výkonu a s převaděči.

(7) Stanice pracující v pásmech *c* a *d* musí být vybaveny automatickou regulací výkonu, která průměrně poskytuje činitel potlačení rušení alespoň 3 dB oproti maximálnímu povolenému výstupnímu výkonu uvedených systémů. Není-li automatická regulace výkonu použita, snižuje se maximální povolený střední e.i.r.p. a odpovídající mez střední hustoty e.i.r.p. pro pásma 5250–5350 MHz a 5470–5725 MHz o 3 dB.

(8) Stanice pracující v pásmech *c* a *d* využívají technologie potlačení rušení (mitigation techniques) které poskytují alespoň takovou míru ochrany jako požadavky na detekci, provoz a odezvu popsané v normě EN 301 893, aby byl zajištěn provoz slučitelný se systémy rádiového určování. Tyto technologie potlačení musí vyrovnávat pravděpodobnost výběru konkrétního kanálu ze všech dostupných kanálů, aby se v průměru zajistilo téměř rovnoměrné rozprostření zátěže spektra.

(9) Provoz stanic podle tohoto všeobecného oprávnění nemá zajištěnou ochranu proti rušení způsobenému vysílacími rádiovými stanicemi jiné radiokomunikační služby, provozovanými na základě individuálního povolení, nebo i téže radiokomunikační služby provozovanými na základě tohoto všeobecného oprávnění.

---

[2]) Střední ekvivalentní izotropicky vyzářený výkon (e.i.r.p.) je e.i.r.p. po dobhu vysílání, který odpovídá nejvyššímu výkonu, pokud je použita regulace výkonu.

Veškeré kmitočty, na kterých jsou stanice provozovány na základě tohoto všeobecného oprávnění, jsou považovány za sdílené. Případné rušení uživatelé stanic řeší vzájemnou dohodou. Rušení odstraní na své náklady, případně zastaví provoz ten uživatel, který uvedl do provozu stanici způsobující rušení později.

(10) Toto všeobecné oprávnění se vztahuje pouze na stanice, které splňují požadavky dané nařízením vlády č. 426/2000 Sb., kterým se stanoví technické požadavky na rádiová a na telekomunikační koncová zařízení [3]).

(11) Konstrukce stanic nesmí být elektricky ani mechanicky měněna.

(12) Stanice podléhají výkonu státní kontroly elektronických komunikací podle § 113 zákona. Uživatelé musí umožnit pověřeným zaměstnancům Úřadu přístup ke stanicím za účelem kontroly a poskytnout odpovídající součinnost podle zákona č. 552/1991 Sb., o státní kontrole, ve znění pozdějších předpisů.

(13) Pověření zaměstnanci Úřadu mohou v případě nedodržení předepsaných parametrů u jednotlivých stanic, nedodržení podmínek tohoto všeobecného oprávnění nebo při rušení rádiového provozu vydat uživatelům podle § 100 odst. 6 zákona rozhodnutí k odstranění závad nebo v odůvodněných případech předběžné opatření k okamžitému odstavení zdroje rušení.

(14) Harmonizovaná norma pro stanice podle tohoto všeobecného oprávnění je ČSN ETSI EN 300 328 (pásmo *a*), ČSN ETSI EN 301 893 (pásma *b, c, d*).

(15) Ke dni vydání tohoto všeobecného oprávnění je harmonizováno provozování ve všech členských státech EU (zařízení „třídy 1") pro stanice pracující v pásmu *a* (2400–2483,5 MHz) s výkonem do 10 mW e.i.r.p. a pro stanice pracující v pásmu *a* (pouze v rozmezí 2400–2454 MHz) s výkonem do 100 mW e.i.r.p.

Článek 3
Závěrečná ustanovení

(1) Dnem účinnosti tohoto všeobecného oprávnění se zrušuje generální licence č. GL–12/R/2000, č.j. 502446/2000–613, ze dne 6. září 2000, ve znění změny č. 1, č.j. 5373/2002–12–613, ze dne 31. května 2002, změny č. 2, č.j. 21526/2002–613, ze dne 7. ledna 2003 a změny č. 3, č.j. 11168/2004–613, ze dne 30. března 2004.

(2) Toto opatření obecné povahy nabývá účinnosti patnáctým dnem ode dne uveřejnění v Telekomunikačním věstníku.

(3) Toto opatření obecné povahy platí do 31. prosince 2010.

---

[3]) Za takové stanice se považují rovněž stanice, u nichž Úřad rozhodl o schválení rádiového zařízení podle § 10 zákona č. 151/2000 Sb., o telekomunikacích a o změně dalších zákonů, ve znění pozdějších předpisů, pokud tyto stanice byly uvedeny na trh před 1. 4. 2003.