

Pomoc pre správcov sietí

zahrňuje
802.11b

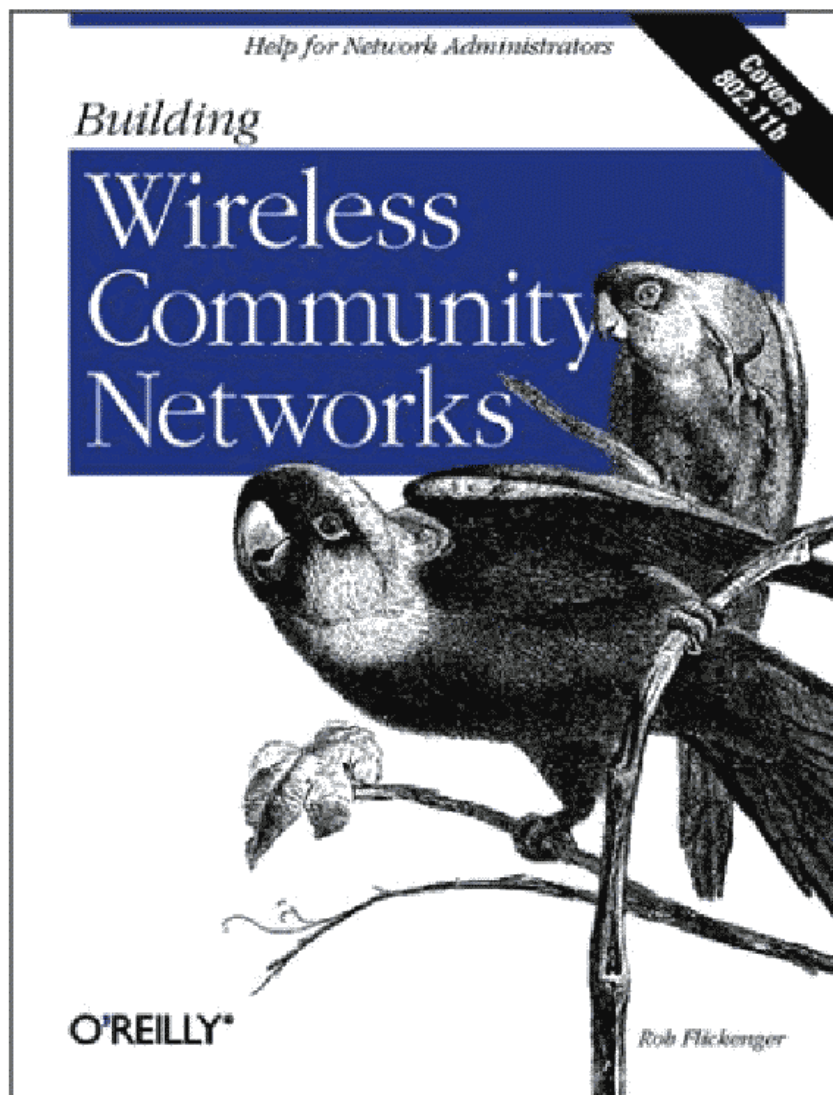
Budujte

Bezdrôtové Komunitné Siete



O'REILLY®

Rob Flickenger



Budujte bezdrôtové komunitné siete
(*Building Wireless Community Networks*)

Rob Flickenger
Preložil: Igor Meltzer
Vydavateľ: O'Reilly

Prvé vydanie, január 2002
ISBN: 0-596-00204-1, 138 strán
SKfree.NET, 91 strán

Kniha „*Budujte bezdrôtové komunitné siete*“ poskytuje zaujímavý návod na výstavbu bezdrôtových sietí na miestnej úrovni: Nie je to drahé a môže to byť realizované a spravované komunitou, ktorá to používa, či už je to škola, susedia, alebo malá firma. Táto kniha poskytuje všetky potrebné informácie pre naplánovanie siete, obstaranie všetkých nevyhnutných komponentov a pochopenie protokolov, ktoré potrebujete pre navrhnutie a realizovanie Vašej siete.

Obsah

Predslov.....	5
Úvod.....	5
Usporiadanie.....	5
Typografické zásady.....	6
Poďakovanie.....	7
Kapitola 1. Bezdrôtové komunitné siete.....	8
1.1 Problém.....	9
1.2 Ako sa ISP pokúšajú o riešenie.....	9
1.3 Ako to robia družstvá.....	11
1.4 O tejto knihe.....	12
Kapitola 2. Definovanie rozsahu projektu.....	13
2.1 Hardvérové požiadavky.....	14
2.1.1 Obhliadka stanovišťa.....	14
2.2 Hot Spots.....	15
2.3 Oblasti s prípadným problémom pokrytia.....	16
2.4 Topografické mapy 101.....	17
Kapitola 3. Štruktúra siete.....	18
3.1 Bezdrôtová infraštruktúra: katedrála verzus bazár.....	18
3.1.1 Hardvér prístupových bodov (AP).....	19
3.1.2 Vytvorenie siete peer-to-peer.....	20
3.2 Dôležité služby.....	21
3.2.1 DHCP.....	21
3.2.2 DNS.....	22
3.2.3 NAT.....	22
3.3 Bezpečnostné aspekty.....	24
3.3.1 WEP.....	25
3.3.2 Smerovanie a firewalling.....	26
3.3.3 Šifrované tunely.....	26
3.4 Zhrnutie.....	28
Kapitola 4. Používanie prístupových bodov - Access Point (AP).....	28
4.1 AP upozornenia.....	29
4.2 Apple AirPort základňa.....	31
4.2.1 Ovládací softvér prístupového bodu.....	31
4.2.2 Lokálny prístup k LAN.....	32
4.2.3 Konfigurovanie vytáčania – dial-up.....	33
4.2.4 NAT a DHCP.....	33
4.2.5 Premosťovanie - Bridging.....	34
4.2.6 WEP, MAC filtrovanie a uzavreté siete.....	35
4.2.7 Roaming.....	36
4.2.8 Odstup kanálov.....	36
Kapitola 5. Peer-to-Peer (Ad-Hoc) sieť.....	37
5.1 Stavba bezdrôtovej brány pod Linuxom.....	37
5.1.1 Hardvér.....	37
5.1.2 Linuxové distribúcie.....	39
5.1.3 Konfigurácia jadra.....	39
5.1.3.1 Linux 2.2.19.....	40
5.1.3.2 Linux 2.4.5.....	40
5.1.4 PCMCIA-CS.....	42
5.1.4.1 Softvér.....	42
5.1.4.2 Konfigurácia.....	42
5.1.5 Wireless Tools (bezdrôtové nástroje).....	44
5.1.6 Maškaráda.....	45
5.1.7 DHCP služby.....	46
5.1.8 Bezpečnosť.....	47
5.1.9 Spájanie všetkého dohromady.....	48
5.1.10 Predpripravené Linuxové Distribúcie.....	49

Kapitola 6. Nasýtenie rozľahlých sietí.....	49
6.1 Topo Maps 102: Vysporiadanie sa s geografickou rozmanitosťou.....	50
6.1.1 Softvér.....	50
6.1.2 Používanie GPS na záznam prípadných Lat/Lon/Alt.....	51
6.1.3 Vykresľovanie bodov do 3D mapy.....	52
6.2 Charakteristiky antén a ich umiestnenie.....	53
6.2.1 Antény.....	55
6.2.1.1 Vsesmerovka - Omni.....	55
6.2.1.2 Sektorová.....	56
6.2.1.3 Yagi.....	56
6.2.1.4 Parabolický tanier.....	57
6.2.1.5 Káble.....	58
6.2.2 Konektory.....	59
6.2.3 Výpočet dosahu.....	62
6.3 Zosilňovače a zákony.....	64
Kapitola 7. Ďalšie aplikácie.....	65
7.1 Spoj bod-bod.....	65
7.2 Obal od Pringles.....	67
7.2.1 Zoznam súčiastok.....	68
7.2.2 Potrebné náradie.....	68
7.2.3 Konštrukcia predného kolektora.....	68
7.2.4 Príprava obalu.....	69
7.2.5 Konštrukcia elementu.....	69
7.3 Zdvojené spoje.....	71
7.4 Repeatre.....	72
7.4.1 Dve karty v jednom PC.....	73
7.4.2 Dva AP Back-to-Back (chrbtom k sebe).....	74
7.5 Starosť o bezpečnosť.....	74
7.5.1 Nadviazanie spojenia.....	75
7.5.2 Nakonfigurujte Váš mailový softvér.....	75
7.6 Captive „Catch and Release“ Portal	76
7.7 Na záver.....	79
Kapitola 8. Radio Free Planet.....	79
8.1 Bezdrôtový Seattle.....	79
8.2 BAWUG.....	80
8.3 Personal Telco.....	80
8.4 NYC Wireless.....	80
8.5 GBPPR.....	81
8.6 GAWD.....	81
8.7 Guerrilla.net.....	81
8.8 Universal Wireless.....	82
Kapitola 9. Radio Free Sebastopol.....	82
9.1 OSCON 2000.....	82
9.1.1 Areál.....	83
9.1.2 Káva, káva, káva.....	83
9.1.3 Online z domu, bez špeciálnych podmienok.....	84
9.1.4 Bezdrôtový Seattle.....	84
9.1.5 NoCat (bez mačky).....	85
9.1.6 Článok.....	86
9.1.7 Summit v Portlande.....	87
9.1.8 Budúcnosť.....	87
Príloha.....	89
A.1 Výpočet straty cestou (Path Loss Calculations).....	89
A.2 Odkazy na stránky bezdrôtových komunit.....	89
A.3 FCC Part 15 Rules.....	90
A.4 Jednoduché spravovanie schém.....	90
Tiráž.....	91
Pár poznámok k prekladu.....	92

Predslov

Kniha „*Budujte bezdrôtové komunitné siete*“ je o vzájomnom spájaní sa ľudí. Bezdrôtová technológia sa práve teraz používa na pripojenie susedov, firiem a škôl do rozsiahleho, masívneho spojenia a hmlistého celku, známeho ako Internet. Jeden z cieľov tejto knihy je pomôcť Vám, aby sa Vaša komunita „odstrihla“ a bola online, použitím nie drahých, hotových zariadení, ktoré možno kúpiť v obchode.

Druhý, ale veľmi dôležitý cieľ tejto knihy je vysvetliť čo presne znamená *komunita*. Môže sa tým myslieť areál vysokej školy, kde má veľa ľudí ich vlastný laptop a chcú zdieľať súbory a prístup na Internet. Vaša predstava komunity môže zahŕňať Váš obytný dom, alebo susedstvo, kde dokonca nemusí byť k dispozícii širokopásmový prístup na Internet. Táto kniha chce, aby ste premýšľali nad tým, čo to znamená, že sú ľudia vo Vašej komunite spojený a tiež obsahuje fungujúce príklady, ako toto spojenie uskutočniť.

Úvod

Táto kniha popisuje niektoré riešenia aktuálneho (ale rýchlo sa meniaceho) problému výstavby bezdrôtových sietí využívaných komunitou. *Nie* je zamýšľaná ako konštrukčná príručka pre bezdrôtové spoločnosti a ISP, aj keď dúfam, že aj oni tu nájdu užitočné informácie (a prinajmenšom trochu zábavy).

Táto kniha je určená pre technických užívateľov, ktorí sa zaujímajú o sprístupnenie bezdrôtového, vysoko rýchlostného, sieťového prístupu všade, kde je požadovaný. To môže zahŕňať rozšírenie Internetového spojenia do oblastí, kde iný prístup (ako DSL, alebo káblovka) nie je. Taktiež môže obsahovať vybudovanie prístupu v škole, ktorej múry boli postavené dávno predtým než ktokoľvek rozmýšľal o ťahaní káblov a prípojok do tried. Táto kniha by tiež mala byť užitočná pre ľudí, ktorých zaujíma, ako tucty skupín po celej Zemi poskytujú bezdrôtový prístup v ich vlastných komunitách. Životný príbeh bezdrôtového sieťového prístupu je ešte stále v období detstva, ale už je plný úchvatných zvrátov a zmien (nehovoriac o jeho možnostiach!). Dúfam, že Vám poskytnem to, čo som sa naučil o tomto príbehu ja.

Usporiadanie

Prvé kapitoly tejto knihy uvádzajú základné bezdrôtové pojmy a základné sieťové služby, zatiaľ čo neskoršie kapitoly sa zameriavajú na špecifické aspekty budovania Vašej vlastnej bezdrôtovej siete. Pokročilí užívatelia budú asi radšej preskakovať medzi kapitolami, než čítať túto knihu rad radom, preto je tu prehľad každej kapitoly:

- **Kapitola 1**, prináša krátku históriu stavu bezdrôtového pripojenia a nejaké predstavy (a varovania) o tom, ako to môže pokračovať.
- **Kapitola 2**, je prehľad viacerých dôležitých logistických rozhodnutí, ktoré budete musieť urobiť pri návrhu Vašej vlastnej siete, popisuje nejaké nástroje, ktoré Vám môžu uľahčiť Vašu prácu.
- **Kapitola 3**, poskytuje detailný popis kritických sieťových komponentov, ktoré budete potrebovať poskytnúť Vaším užívateľom. Štruktúra siete a bezpečnosť sú tiež spomenuté.
- **Kapitola 4**, detaily ako efektívne používať bezdrôtový prístupový bod (AP).
- **Kapitola 5**, je príručka, typu krok za krokom, ako vybudovať Váš vlastný AP s použitím Linuxu, nie drahého PC hardvéru a bežných bezdrôtových kariet.

- [Kapitola 6](#), je o rozširovaní Vášho dosahu. Pozerá sa na používanie mapového softvéru pri vyhodnocovaní spojov na dlhé vzdialenosti a tiež sa zmieňuje o spuste antén, káblov a konektorov, ktoré zaiste stretnete. Taktiež poskytuje jednoduchú metódu výpočtu použiteľného dosahu Vášho zariadenia.
- [Kapitola 7](#), preskúmava niektoré naozaj exotické (a užitočné !) aplikácie 802.11b. To zahrňuje praktické návody pre zostavenie spojov z bodu do bodu, nejaké jednoduché repeatre (opakovače), výrobu 2.4GHz antény z bežných predmetov z domácnosti a veľa ďalších zábavných výskumov. Tiež to zahrňuje implementáciu dynamického firewallu „captive portal“ (uväzňovací portál) použitím open source softvéru (softvér s otvoreným zdrojovým kódom).
- [Kapitola 8](#), je sprievodca ku niektorým hlavným aktérom revolúcie bezdrôtového sieťového prístupu. Tu nájdete, ako ľudia po celom svete realizujú myšlienku všadeprítomného bezdrôtového sieťového prístupu, všetko vo svojom voľnom čase.
- [Kapitola 9](#), je (krátka) história mojich vlastných skúseností pri budovaní verejného bezdrôtového Internetového prístupu v Sebastopol-e, CA (a o stretnutiach priamo s vedením niektorých najväčších komunít v USA).
- Nakoniec, [Príloha A](#), poskytuje tabuľku vypočítaných strát cestou, kópiu predpisu FCC Part 15 a niektoré ďalšie užitočné dodatky.

Typografické zásady

V tejto knihe sú použité nasledujúce typografické zásady:

Kurzíva

Použité na predstavenie nových termínov, označenie URL, premenných, alebo užívateľom definovaných súborov a adresárov, príkazov, prípon súborov, názvov súborov, názvov adresárov a UNC ciest.

Kurzíva s pevnou šírkou

Použité na zobrazenie premenných, ktoré by mali byť príslušne nahradené podľa kontextu.



Označuje tip.



Označuje varovanie.

Pod'akovanie

Chcel by som sa poďakovať sieťovému tímu O'Reilly, mojím rodičom a obzvlášť Cat, za ich nekončiace povzbudzovanie a udržovanie ma pri rozume (a v niektorých prípadoch dokonca pri vedomí).

Moje úprimné poďakovanie patrí tiež tým, ktorí pomáhali premeniť myšlienku NoCat na skutočný živý projekt, sú to Schuyler Erle, Adam Flaherty, Nate Boblitt a Jim Rosenbaum. Rovnako ďakujem aj týmto: Matt Peterson, Matt Westervelt Adam Shand, Terry Shmidt a bezpočtu ďalších priekopníkov ultra-hyper-pripojenia.

Vďaka za prezeranie, čítanie prvých konceptov a tvorbu pripomienok patrí aj nasledovným: Mike Bertsch, Simon Garfinkel, Justin Lancaster, Nicholas Maddix a Matt Peterson. Ďakujem aj ľuďom z O'Reilly & Associates, ktorí premenili tento rukopis na konečnú knihu: Sue Miller - editor, Leanne Soylemez - výrobný editor, Rob Romano - grafik, Catherine Morris - copyeditor a Mary Anne Weeks Mayo - kontrola kvality.

Kapitola 1. Bezdrôtové komunitné siete

V nedávnych časoch, rýchlosť vývoja technológií dosiahla kozmickú rýchlosť a teraz sa pohybuje rýchlosťou, ktorá sa nedá opísať. Obzvlášť Internetová technológia urobila ohromný pokrok v niekoľkých posledných rokoch. Keď len pred niekoľkými málo rokmi boli 56Kb modemy veľkou vymoženosťou, dnes veľa technikov sa sťažuje na to, aké pomalé sa zdá byť T1 pripojenie ich firmy, v porovnaní s ich 6Mb DSL pripojením doma.

Nikdy predtým nemalo tak veľa ľudí voľný a rýchly prístup k tak veľa informáciám. Aj keď mnoho ľudí okúsilo čas odozvy v milisekundách a rýchlosť sťahovania v megabitoch zdá sa, že chcú ešte viac. Na mnohých miestach, služba po ktorej všetci túžia je *DSL*, alebo *Digital Subscriber Line*. Poskytuje veľkú šírku pásma (obvykle, niekde od 384Kbps po 6Mbps) pri bežnej medenej telefónnej linke, ak je Vaša inštalácia v okruhu do cca. troch míľ od telefónnej centrály (to je technické obmedzenie technológie). DSL je obvyčajne uprednostnené pred káblovými modemami, pretože DSL pripojenie poskytuje garantovanú šírku pásma (prinajmenšom po telefónnu spoločnosť) a tak nie je priamo ovplyvnené správaním sa susedov pri prenášaní dát po sieti (traffic). Nie je to lacné, cena sa pohybuje v intervale od 50 USD po 300 USD za mesiac, plus poplatky ISP a za zariadenia, ale nezdá sa to byť odstrašujúca požiadavka.

Samozrejme, telefónne spoločnosti sú úplne okúzlené touto situáciou. V skutočnosti, veľký dopyt na veľmi-širokopásmový sieťový prístup podnietil taký rozmach obchodu, že dlhé dodacie lehoty inštalácie DSL sú teraz pravidlom v mnohých častiach krajiny. V mnohých oblastiach, ak bývate za hranicou telefónnej ústredne, dodacia lehota je uvedená od dvoch do troch rokov (obchodný žargón na „nikdy, ale každopádne zoberieme Vaše peniaze, ak chcete“). Horšie než to, pri nastupujúcej rozsiahlej konsolidácii trhu, niektorí zákazníci, ktorí boli celkom spokojný s ich DSL službami, stroskotali keď ich miestny ISP skončili s činnosťou¹.

Aká je alternatíva pre ľudí, ktorí chcú vysoko rýchlostný Internetový prístup, ale nechcú čakať kým spoločnosti ponúknu pre nich vhodné riešenie? Telefónne spoločnosti vlastnia med' a káblové spoločnosti vlastnia koaxiál.

Bezdrôtové siete teraz poskytujú jednoduché, nedaré, vysoko-širokopásmové sieťové služby pre každého, kto má záujem ich nastaviť.

Inštitúcia IEEE Standards Committee schválila v roku 1997 špecifikáciu 802.11, ktorá popisuje štruktúru potrebnú pre štandardnú metódu bezdrôtovej sieťovej komunikácie. Využíva mikrovlnné pásmo 2.4GHz, navrhnuté pre nízke výkony, ktorého používanie od roku 1985 nie je podľa FCC v USA licencované. 802.11 umožňuje sieťovú rýchlosť jeden, alebo dva megabity, pri použití jednej z dvoch nekompatibilných dekódovacích schém: Frequency Hopping Spread Spectrum (FHSS) a Direct Sequence Spread Spectrum (DSSS).

V septembri 1999, výbor 802 rozšíril danú špecifikáciu a rozhodol o štandardizácii založenej na DSSS. Toto rozšírenie, 802.11b, umožňuje nové, omnoho exotickéjšie dekódovacie techniky. To posunulo priepustnosť na oveľa úctyhodnejších 5.5, alebo 11Mbps. Hoci došlo k prerušeniu kompatibility so schémou FHSS, rozšírenie umožnilo novým zariadeniam spolupracovať so starším 802.11 DSSS hardvérom. Technológia bola zamýšľaná na poskytovanie „areálového“ prístupu k sieťovým službám, pričom ponúkala typický použiteľný dosah približne 1500 stôp.

¹ Jedna aktuálne rezonujúca spomienka na tento fenomén označuje stroskotaných DSL zákazníkov „Northpoint-ovanými“, na počesť ISP NorthPoint.net, ktorý sa dostal do problémov minulý marec, pričom zanechal tisíce ľudí bez prístupu.

Niektorým ostrým hackerským typom (a v skutočnosti aj pár CEO a FCC typom) netrvalo dlho, kým sa im podarilo použitím 802.11b klientských zariadení v spojení so štandardným rádiovým zariadením rozšíriť efektívny dosah na viac ako dvadsať míľ a teoreticky poskytnúť tisícom ľudí šírku pásma, dosahujúcu rýchlosť DSL, pri minimálnej cene hardvéru. Pripojenie, ktoré sa predtým muselo plaziť cez monopolne držané drôty, môže teraz prilietieť cez steny, s významne vyššou výkonnosťou. A odkedy 802.11b využíva nelicencované rádiové spektrum, časovo neobmedzené pripojenie môže byť vytvorené *bez zaplattenia koruny za strávený čas, alebo licenčných poplatkov*.

Aj keď tromfnutie telekomunikačných a káblových spoločností zakúpiteľným magickým hardvérom môže byť zábavná fantázia, ako dobre v skutočnosti slúžia 802.11b zariadenia v reálnom svete? Ako môžu byť efektívne aplikované, aby poskytovali prístup na Internet?

1.1 Problém

Očividné určenie 802.11b je poskytovať smutne známe sieťové služby „poslednej míle“. Tento termín sa vzťahuje na vzdialenosť medzi tými, ktorí majú dobrý prístup na Internet (ISP, telekomunikačné a káblové spoločnosti) a tými, ktorí ho chcú (zákazníci). Tento druh usporiadania vyžaduje 802.11b zariadenia na oboch koncoch (napríklad, na strane ISP i u zákazníka doma).

Nanešťastie, povaha rádiovkej komunikácie na mikrovlnných frekvenciách požaduje *priamu viditeľnosť (line of sight)* pre optimálnu výkonnosť. To znamená, že by mal byť výhľad, bez prekážok, medzi danými dvoma anténami, pokiaľ možno nič, len údolie medzi nimi. To je absolútne kritické pri aplikáciách na dlhé vzdialenosti s nízkym výkonom. Rádiové vlny prenikajú mnohými bežnými materiálmi, ale dosah sa významne znižuje pri prechode hocičím iným ako vzduch. Hoci zvýšenie vysielačeho výkonu môže pomôcť dostať sa cez stromy a iné prekážky, jednoduché pridanie zosilňovačov nie je vždy možné, keďže FCC predpisuje prísne limity na výkon. (Vid' [príloha A](#), kópia pravidiel FCC Part 15, ktoré sa vzťahujú na 2.4GHz emisie. Podrobnejšie sa k tomu vrátíme v [kapitole 7](#).)

Keď už hovoríme o zosilňovačoch, súvisiaca technická prekážka, s ktorou sa treba vysporiadať pred dosiahnutím bezdrôtovej nirvány, je šum v pásme. Pásmo 2.4GHz nie je rezervované na výhradné použitie 802.11b zariadeniami. Musia zdieľať pásmo s mnohými ďalšími zariadeniami, vrátane bezdrôtových telefónov, bezdrôtových X-10 kamier, Bluetooth zariadení, poplašných zariadení a dokonca mikrovlnných rúr! Použitie zosilňovačov na to, aby ste si „prerazili“ cestu cez vyskytujúce sa prekážky a napriek šumu v pozadí, má spoločenský ekvivalent pridania hlasitosti televízie na plno, tak že ju môžete počuť aj vonku pred dverami (možno tiež, aby ste ju počuli napriek Vášmu zvoniacemu telefónu, štekajúcemu psovi, alebo dokonca hlasnej televízii Vášho suseda, ...).

Ak majú dáta voľne lietieť vzduchom, musí tam byť vysoký stupeň koordinácie medzi tými, ktorí to nastavujú. Keďže vzduchové vlny sú verejné zdroje, bezdrôtová infraštruktúra by mala byť vybudovaná tak, aby bola prospešná najviac ľuďom ako je možné, pri čo najnižšej cene. Ako môže 802.11b efektívne spájať ľudí navzájom?

1.2 Ako sa ISP pokúšajú o riešenie

V týchto dňoch určite tancuje v hlavách niektorých obchodne zmýšľajúcich jedincov predstava sietí bez potreby licencie, rozbíjajúcich monopol, vysoko-širokopásmových. Navonok to vyzerá logicky: ak sú ľudia vycvičení veriť, že poskytovanie

6Mb DSL stojí 250 USD za mesiac, potom určite budú ochotný platiť prinajmenšom rovnako veľa za 11Mb bezdrôtové pripojenie, ktorého prevádzka stojí haliere, obzvlášť, ak je to šikovne zaobalené ako upgrade pod obchodnou značkou, ktorú už poznajú. Zdá sa, že pokúšenie vysokého zisku a nízkych prevádzkových nákladov opäť raz umožnilo obchodovanie. Tak sa zrodil fenomén bezdrôtového DSL. (Mimochodom, kto potrebuje vlastnú technológiu, keď môžete predávať skratku?)

V skutočnosti, mnoho WISP² zisťuje, že to nie je tak jednoduché, ako nahodenie nejakých antén a hrabanie hotovosti. Aby sa s tým dalo začať, pravé DSL poskytuje plne duplexnú, prepínanú linku. Veľa DSL liniek je asymetrických, čo znamená, že umožňujú vyššie rýchlosti pri sťahovaní za cenu nižších rýchlostí pri odosielaní. Tento rozdiel je sotva badateľný keď najviac sieťového prenosu (traffic) je prichádzajúceho (napr.: keď si užívatelia prezerajú Web), ale rozdiel skutočne je. Dokonca aj s obmedzením nízkou rýchlosťou odosielenia, plne duplexná linka dokáže odosielať a prijímať dáta súčasne. Potenciálny bezdrôtový poskytovateľ, ktorý stavia na technológiu 802.11b, je obmedzený spojením s polovičným duplexom pri zdieľanej šírke pásma. To znamená, že aby poskytoval rovnakú kvalitu služieb ako drôtová DSL linka, potreboval by štyri rádiá pre každého zákazníka: dva na každý koniec, jedno na odosielanie a jedno pre sťahovanie. Ak plánom sieťovej infraštruktúry je poskytovať zopár (alebo dokonca zopár tuctov) miest s bezdrôtovým prístupom po celom meste, potrebovali by byť zdieľané všetkými užívateľmi, čo by neskôr znižovalo výkonnosť siete, presne ako nočná mora káblového modemu. Dodatočné prístupové miesta by mohli pomôcť, ale pridanie zariadení tiež zvyšuje hardvérové a prevádzkové náklady.

Keď hovoríme o AP, kde presne by mali byť umiestnené? Prirodzene, antény by mali byť umiestnené všade tam, kde na ne vidí najväčšia časť očakávaných zákazníkov. Ak ste si to ešte nevyskúšali, garantujem Vám, že je to ťažšie ako sa zdá. Stromy, kovové konštrukcie, ploty a prirodzený tvar krajiny sú pri umiestňovaní antény zaujímavou výzvou pre ľudí, ktorí to berú ako hobby, ale nočnou morou pre sieťových inžinierov. Ako neskôr uvidíme, bežné miesto pre anténu potrebuje napájanie, pevný stožiar na upevnenie zariadenia a pokiaľ možno má tiež prístup ku káblovej chrbtici. Inak by dokonca bolo potrebných viac rádii na poskytovanie sieťových služieb vo veži.

Pripusťme, že marketing skutočne nachytá potenciálnych zákazníkov a obsadí dostatok miest na vežiach tak, že poskytovať sieťové služby bude prinajmenšom možné. Teraz si predstavme, že prípadný zákazník skutočne zavolá s požiadavkou na služby. Ako bude WISP vedieť či je služba možná? Pri DSL je to jednoznačné: vyhľadať telefónne číslo zákazníka v centrálnej databáze, zistiť ako ďaleko je od ústredne a dať mu vyhodnotenie. Žiaľ, žiadna známa databáza Vám s určitosťou nepovie či je na zadanú adresu priama viditeľnosť.

Ako uvidíme neskôr, topografický softvér môže vykonať nejaké prípravné práce a pomôcť odmietnuť prinajmenšom určite nemožné požiadavky. Niektoré topografické balíky dokonca obsahujú stromy a rušivé zóny. V tomto bode môžeme byť dokonca schopný povýšiť potenciálneho zákazníka na „snáď“. Avšak napokon jediný spôsob ako sa dozvedieť, či príslušný zákazník dosiahne chrbticu WISP cez bezdrôt, je vyslať technika s testovacím zariadením a vyskúšať to.

Tak, teraz chudák WISP potrebuje armádu technicky zdatných ľudí, s autami, na telefóne, ktorí pri požiadavke na služby, vykonajú na mieste preverenie u ľudí, ktorí dokonca ešte ani nie sú ich zákazníci. A ak majú šťastie, možno sa im podarí sprevádzkovať testovacie spojenie, zariadenie môže byť definitívne nainštalované, zmluva

2 Wireless Internet Service Provider (bezdrôtový poskytovateľ Internetových služieb). Nie, ja som nič také nevytvoril.

podpísaná a zákazník môže byť online s niečím takmer sa podobajúcim na DSL. A je to, zákazník môže byť online, dokiaľ si nesaďne na anténu vták, alebo na trase nevyrastie nová budova, alebo na jar nevypučia listy a nezablokujú väčšinu signálu (myslím si, že zákazník bude odkázaný na klauzuly, napísané malým písmom, na zmluve).

Myslím si, že už začínate presne vidieť, kde je pointa pri tomto type usporiadania. Určite to nie je nikoho chyba, len toto riešenie jednoducho nie je ušité na tento problém, pretože jediná jednotka s dostatkom zdrojov na to, aby sa o to skutočne pokúsila, by pravdepodobne mohla byť telefónna spoločnosť. Aké šance má naša vízia „všade bezdrôt“ vo svetle všetkých tých doteraz spomenutých problémov? Možno by pomohol výrazný paralelný spôsob ...

1.3 Ako to robia družstvá

Problémy komerčného spôsobu realizácie bezdrôtového prístupu existujú kvôli jednému sociálnemu fenoménu: zákazník si nakupuje riešenie a preto očakáva za svoje peniaze primerané služby. Pri komerčnom podnikaní napokon WISP zodpovedá za dodržanie zmluvy, v opačnom prípade musí kompenzovať zákazníkov.

Problém „poslednej míle“ získa úplne iný rozmer, ak každý člen siete zodpovedá za držanie svojho vlastného zariadenia online. Rovnako ako mnoho nápadov, ktorých čas prichádza, fenomén komunitných bezdrôtových sietí sa práve teraz rozvíja po celom svete³. Ľudia, ktorí majú plné zuby dlhých termínov a vysokých cien za zariadenia a inštaláciu spájajú svoje zdroje, aby poskytl bezdrôtový prístup svojim priateľom, rodine, susedom, školám a odľahlým miestam, ktoré inak určite nikdy neuvidia širokopásmový prístup. Taká ťažká, ako príklad nočnej mory WISP, je aj táto myšlienka, všade sa ľudia učia, že nemusia nevyhnutne platiť poplatky telekomunikáciám, aby zrealizovali prekvapivé veci. Objavujú, že je naozaj možné poskytovať pripojenie s veľmi veľkou šírkou pásma tým, ktorí ho potrebujú, za pence – a nie za tisíce dolárov – mesačne.

Samozrejme, ľudia od ktorých sa očakáva, že budú prevádzkovať bezdrôtovú bránu, potrebujú prístup buď ku vysoko technickým informáciám, alebo riešenie, ktoré nie je oveľa ťažšie, než zasunutie konektora a preklopenie vypínača. Hoci dávanie spoločných skúseností dohromady môže pomôcť nájsť jednoduché riešenie omnoho rýchlejšie, len relatívne malé percento ľudí na svete vôbec vie, že mikrovlnná komunikácia je možná. Ešte menej vie ako efektívne pripojiť bezdrôtovú sieť k Internetu. Ako uvidíme neskôr, všadeprítomnosť je kritická požiadavka, ak sa pripravuje bezdrôtový prístup pre rozľahlú oblasť. Je v každeho najlepšom záujme spolupracovať, zdieľať čo vie a pomáhať poskytovať šírku pásma, aby bola tak samozrejmalá, ako vzduch, ktorý dýchame.

Túžba ukončiť rozdiely medzi „tými ktorí vedia“ a „tými ktorí chcú vedieť“ pomáha dostať ľudí preč od ich počítačových obrazoviek, späť do ich blízkeho susedstva. V poslednom roku sa sformovali tucty nezávislých lokálnych skupín s veľmi podobnými základnými princípmi: pripojiť navzájom toľko ľudí koľko je možné za najnižšiu možnú cenu. Web stránky, diskusné skupiny, komunitné stretnutia a dokonca IRC kanály vznikajú, aby poskytovali informácie o existujúcich bezdrôtových sieťových prístupoch pre tých, ktorí to potrebujú. Všade kde sa dá, vznikajú dômyselné, jednoduché a nedarhé (avšak výkonné) návrhy. Tisíce ľudí pracujú na tomto probléme, nie pre osobný zisk, ale pre osoh celej planéty.

³ GAWD (Global Access Wireless Database), obsahuje 198 verejných bezdrôtových AP v čase písania tejto knihy. Pozrite si <http://www.shmoo.com/gawd/> a pridajte Váš vlastný, alebo si nejaký vyhľadajte.

Je dobré zmieniť sa tu, že ISP a telekomunikácie nie sú žiadnym spôsobom ohrozené touto technológiou, v skutočnosti, Internetové služby budú dokonca väčšmi žiadané, keď budú bezdrôtoví spolupracovníci online. Rozdiel je v tom, že veľa koncových užívateľov bude mať prístup bez potreby stínať stromy a prekopávať ulice a mnoho ďalších možno zistiť, že sieťový prístup v obľúbených oblastiach bude poskytovaný grátis, ako komunitná služba, alebo na základe dôvery spolupracovníkov, radšej než ako komerčný tovar.

1.4 O tejto knihe

Hlavným cieľom tejto knihy je nadchnúť Vás pre túto technológiu a vyzbrojiť Vás informáciami s ktorými potrebujete pracovať vo Vašej komunite. Predstavíme si rôzne techniky a zariadenia pre pripojenie bezdrôtových sietí ku káblovým sieťam a pozrieme sa, ako ostatní „s vedomosťami“ umožňujú svojim susedom, školám a firmám navzájom komunikovať vzduchom. Postupne si ukážeme krajné medze, čo je možné s 802.11b sieťami, ako predĺžiť dosah na míle a spôsoby poskytovania prístupu pre stovky ľudí. Ak Vám Váš rozpočet nevystačí pre všetky sieťové zariadenia, ktoré potrebujete, ukážeme Vám ako si niektoré zostrojíte svojpomocne.

Prostredníctvom úsilia bezpočtu dobrovoľníkov a nadšencov sa mnoho vecí hýbe oveľa lacnejšie a ľahšie než kedykoľvek v minulosti. Práve teraz sa deje v bezdrôtovom svete oveľa viac než je možné skutočne dať na papier. Buďte online a zisťujte čo ostatní vo Vašej oblasti robia s touto technológiou (početné online odvolávky sú uvedené v texte a v [prílohe A](#)).

Dúfam, že bude pre Vás táto kniha užitočným a praktickým nástrojom na ceste ku Vašej vlastnej bezdrôtovej utópii.

Kapitola 2. Definovanie rozsahu projektu

Čo chcete dosiahnuť? To je otázka, ktorú ako systémový administrátor kladiem vždy, keď za mnou príde nejaký užívateľ s novou požiadavkou. Je ľahké sa ponoriť do implementačných detailov, zatiaľ čo zabudnete čo presne ste začali robiť. Keď sa projekt stáva omnoho komplikovanejší ľahko zbadáte, že sa Vaše „kolesá krútia“ bez toho, aby ste sa niekam pohybovali.

Najbežnejšie otázky s ktorými som sa stretol pri 802.11b sieťach sa zdali byť najjednoduchšie:

- Koľko to stojí?
- Aký to bude mať dosah?
- Môžem to použiť na ... [vyplňte vynechané miesto] ?

Samozrejme, na tieto otázky existujú suverénne teoretické odpovede, ale všetky majú jednu rovnakú praktickú odpoveď: „To je rôzne!“. Je jednoduchšie vysvetliť, ako ľudia aplikovali bezdrôt na to, aby dosiahli svoje potreby a odpovedať na tieto otázky vysvetlením na príkladoch.

Ľudia používajú 802.11b siete tromi hlavnými spôsobmi: *spoje z bodu do bodu (bod-bod)*, *spoje bod-multibod* a *ad-hoc (alebo peer-to-peer) pracovné skupiny*. Typická aplikácia bod-bod by bola poskytovanie šírky pásma siete tam, kde by inak nebola dostupná. Napríklad, predstavme si, že máte DSL linku vo Vašej kancelárii, ale nemôžete ju mať inštalovanú doma (kvôli limitu vzdialenosti od ústredne). Ak máte z Vašej kancelárie nerušený výhľad na Váš dom, pravdepodobne môžete vytvoriť spoj bod-bod na ich vzájomné prepojenie. S vhodnými anténami a pri priamej viditeľnosti môže mať spoľahlivý spoj bod-bod nad 20 míľ (pri až 11Mbps!).

Jeden z bežných spôsobov použitia bezdrôtu spôsobom bod-multibod, je vytvorenie AP doma, aby ste umožnili niekoľkým laptopovým užívateľom súčasne prezeráť Internet odkiaľkoľvek (gauč v obývačke je typický príklad). Vždy, keď niekoľko uzlov komunikuje s jediným centrálnym bodom prístupu, je to aplikácia bod-multibod. Ale bod-multibod nemusí končiť doma. Povedzme, že pracujete v škole, ktorá má rýchle Internetové pripojenie v jednej budove, ale ostatné budovy vo Vašom areáli nie sú navzájom skáblované. Radšej než utrátiť tisíce za získanie CAT5, alebo natiahnutie drôtu medzi budovami, môžete použiť AP na Internetovej budove s jednou anténou, ktorú všetky ostatné budovy dokážu vidieť. To by malo umožniť celému areálu zdieľať Internetovú šírku pásma za zlomok ceny kábla a už o pár dní namiesto mesiacov.

Posledná trieda sietí, ad-hoc (alebo peer-to-peer), sa uplatňuje kedykoľvek keď nie je k dispozícii AP. V peer-to-peer móde môžu uzly s rovnakým sieťovým nastavením navzájom komunikovať pokiaľ sú v dosahu. Veľký ošoh z tohto operačného módu je, že dokonca ak ani jeden z uzlov nie je v dosahu centrálného AP, stále môžu navzájom komunikovať. Napríklad, je to ideálne na rýchly presun súborov medzi Vaším a kamarátovým laptopom, keď ste mimo dosahu AP. Na dôvažok, ak jeden z uzlov v dosahu sa stane Internetovou bránou, potom môže byť traffic prenášaný na a z Internetu rovnako, ako keby to bolo tradičné AP. V [kapitole 5](#) uvidíme spôsob použitia tohto módu na poskytovanie služieb brány, bez potreby drahého hardvéru AP. V [kapitole 7](#) na tom postavíme jednoduchú bránu, aby sme vytvorili vrátnika pre bezdrôtový verejný prístup, s dynamickým firewallom, uväzňovacím web portálom, autentifikáciou užívateľa a traffic shaping-om v reálnom čase.

Môžete použiť tento operačný mód v spojení s ktorýmkoľvek iným (a s ďalšími káblowymi sieťovými technikami), aby ste rozšírili Vašu sieť tak, ako to potrebujete. Je to veľmi bežné, napríklad, použiť dlhý bezdrôtový spoj na poskytnutie prístupu odľahlému miestu a následne na konci nastaviť AP, kvôli poskytovaniu lokálneho prístupu.

2.1 Hardvérové požiadavky

Celková cena Vášho projektu závisí predovšetkým na jeho cieľoch a na tom, koľko práce si chcete urobiť sami. Hoci určite môžete minúť desiatky tisíc dolárov za zariadenia triedy ISP, môžete ušetriť peniaze (a získať väčšie zadosťučinenie) ak si to postavíte sami, s obdobnou funkčnosťou, s lacnejším zakúpiteľným hardvérom.

Ak len chcete pripojiť Váš laptop k niekoho iného 802.11b sieti, budete potrebovať iba klientskú kartu a ovládač (kompatibilné karty stoja medzi 50 a 200 USD). Ako aj pri iných zariadeniach, cena obvykle narastá s dodatočnými funkciami, ako sú konektor pre externú anténu, vyšší výstupný výkon, citlivejšie rádio a obvyklé zvončeky a pískanie. Potom čo si vyberiete kartu, zistíte sieťové nastavenie pre sieť ku ktorej sa chcete pripojiť a choďte na to. Ak potrebujete väčší dosah, malá všesmerová anténa (obvykle 50-100 USD) dokáže výrazne rozšíriť dosah Vášho laptopu pre roaming.

Ak chcete poskytovať bezdrôtový prístup ostatným ľuďom, budete potrebovať *prístupový bod* (*access point* - AP). Toto označenie sa stalo zaužívaným termínom a môže sa vzťahovať sa hocičo od amatérskych „brán obydlia“ (cca. 200 USD), po profesionálne, kvalitné, viac rádiové zariadenia (viac ako 1000 USD). Sú to obvykle malé, samostatné krabice, ktoré obsahujú minimálne jedno rádio a ďalšie sieťové pripojenie (ako Ethernet, alebo dial-up modem). V tejto knihe budeme používať termín AP vo vzťahu ku akémukoľvek zariadeniu schopnému poskytovať sieťový prístup Vaším bezdrôtovým klientom. Ako uvidíme v [kapitole 5](#), môže to byť dokonca bežný PC router vybavený bezdrôtovou kartou.

Aj keď rádio a AP dokážu vytvoriť jednoduchú sieť s krátkym dosahom, viac než pravdepodobne budete chcieť rozšíriť Vaše pokrytie za hranice možností krabice. Najefektívnejší spôsob rozšírenia dosahu je použiť externé antény. Existuje obrovský sortiment antén, od malých stolových všesmerových, po veľké montované parabolické taniere. Neexistuje jediná „pravá“ anténa pre všetky aplikácie, budete si potrebovať vybrať anténu, ktorá bude vyhovovať Vaším potrebám (ak sa pokúšate pokryť len jednu budovu, možno ani nebudete potrebovať externú anténu). Pozrite si podrobný popis jednotlivých antén v [kapitole 6](#).

2.1.1 Obhliadka stanovišťa

Najvhodnejšia bezdrôtová sieť pozostáva z jediného klienta komunikujúceho s jediným AP, vzdialeným zopár stôp, pri absolútne čistej priamej viditeľnosti medzi nimi a so žiadnym šumom na používanom kanály (buď od inej siete, alebo zo zariadenia, ktoré zdieľa 2.4GHz spektrum). Samozrejme, okrem prípadnej výnimky domácej bezdrôtovej LAN, tieto ideálne podmienky jednoducho nie sú reálne. Všetci Vaši užívatelia budú musieť „zdieľať vzduchové vlny“ a viac ako pravdepodobne nebudú schopní vidieť AP z miesta kde sa nachádzajú. Našťastie, 802.11b zariadenia sú veľmi tolerantné k menej než optimálnym podmienkam na blízko. Keď plánujete Vašu sieť, určite si dávajte pozor na nasledujúce:

- Objekty, ktoré absorbujú mikrovlnný signál, ako sú stromy, zem, tehly, sadrové steny a ľudia.

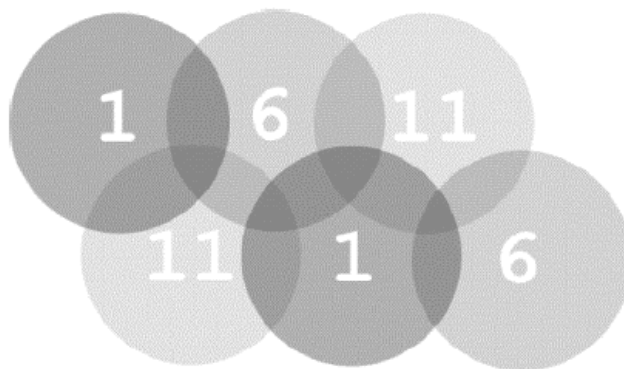
- Objekty, ktoré signál odrážajú, alebo rozptyľujú, ako sú kovy, ploty, potrubia, obrazovky, vodné plochy.
- Zdroje 2.4GHz šumu, ako sú mikrovlnné rúry, bezdrôtové telefóny, bezdrôtové X-10 automatické zariadenia a iné 802.11b siete.

Čím viac toho dokážete odstrániť z trasy medzi Vaším AP a Vašími klientmi, tým šťastnejší budete. Nebudete schopný zbaviť sa všetkých vyššie spomenutých prekážok, ale mali by ste byť schopný minimalizovať ich vplyv, ak sa nimi budete zaoberať.

2.2 Hot Spots

Špecifikácia IEEE 802.11b uvádza 11 možných prekrývajúcich sa frekvencií, na ktorých môže prebiehať komunikácia. Veľmi podobne ako pri bezdrôtovom telefóne, zmena kanála dokáže eliminovať šum, ktorý znižuje výkonnosť siete, a dokonca umožňuje spolužitie viacerých sietí v tom istom fyzickom priestore, bez vzájomného ovplyvňovania sa.

Namiesto pokúšania sa vytvoriť jeden centrálny AP s vysoko ziskovou všesmerovou anténou, pravdepodobne zistíte, že je omnoho efektívnejšie vytvoriť niekoľko prekrývajúcich sa oblastí s kratším dosahom. Ak použijete hardvérové AP a všetky AP sú pripojené na ten istý fyzický sieťový segment, môžu dokonca používatelia súvisle prechádzať medzi oblasťami. *Obrázok 2-1* znázorňuje príklad použitia viacerých AP na pokrytie veľkej oblasti.



Obrázok 2-1. Použité nie susediacich kanálov, niekoľko AP dokáže pokryť veľkú oblasť.

Ako je uvedené v špecifikácii, 802.11b rozdeľuje dostupné spektrum na 11 prekrývajúcich sa kanálov, tak ako je to uvedené v *tabuľke 2-1*.

Tabuľka 2-1. Frekvencie kanálov 802.11b

Kanál	Frekvencia [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

Kanály sú rozprestreté spektrum a skutočne zaberajú 22MHz zo šírky pásma signálu, preto susediace rádiá budú potrebovať byť oddelené minimálne piatimi kanálmi, aby nemali žiadne prekrytie. Napríklad kanály 1, 6 a 11 nemajú žiadne prekrytie. Ani 2 a 7, 3 a 8, 4 a 9, alebo 5 a 10. Hoci budete chcieť používať neprekrývajúce sa kanály pre Vaše AP v preplnenej oblasti (ako sú sídliská, alebo parky) sa to stáva nemožným.

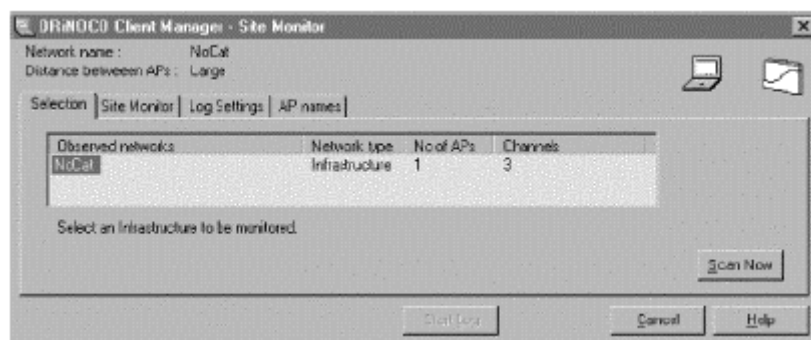
Väčšiu šancu máte pri nasýtení Vašej oblasti použiteľným signálom z viacerých menej výkonných buniek, namiesto jednej veže s vysoko ziskovou anténou. Keďže Vaše jednotlivé bunky nebudú potrebovať obrovský dosah na pokrytie širokej oblasti, môžete použiť antény s nižším výkonom (a nižšou cenou), okrem toho obmedzíte šance na vzájomné ovplyvňovanie sa s ostatnými zariadeniami v pásme. Napríklad, by ste mohli použiť len tri kanály (ako sú 1, 6 a 11) na pokrytie nekonečne veľkej oblasti, bez akéhokoľvek prekrývania sa kanálov.

Najhorší možný prípad nastáva, keď dve nezávislé, vyťažené siete, nachádzajúce sa hneď vedľa seba, sa pokúšajú obsadiť ten istý kanál. Čím ďalej sa môžete dostať od tejto nočnej mory kolízií, tým lepšie. Realisticky, jeden kanál dokáže ľahko podporovať päťdesiat, alebo viac súbežných používateľov a primerané množstvo prekrytia kanálu je znesiteľné. Rádia využívajú vzduch len vtedy, keď skutočne niečo prenášajú a automaticky znovu-prenášajú pri chybe, takže silné preťaženie sa javí koncovému užívateľovi viac menej ako obyčajné sieťové omeškanie (net lag). Náhodný charakter väčšiny sieťového prenosu pomáha zdieľať vzduch a vyhýbať sa kolíziám, podobne ako pri miešaní balíčka hracích kariet.

Úplnú kontrolu môžete mať nad svojím vlastným AP, ale čo Vaši susedia? Ako môžete vedieť, ktoré kanály sú používané vo Vašej oblasti?

2.3 Oblasti s prípadným problémom pokrytia

Hoci spektrálny analyzátor (a inžinier na obsluhu) je dokonalý merací nástroj, takáto vec nie je lacná. Našťastie, môžete získať veľa užitočných informácií použitím dobrého, kvalitného rádia a softvéru. Pozrite sa na nástroje, ktoré ste dostali s Vaším bezdrôtovým zariadením (nástroj od firmy Lucent, Site Monitor, zobrazený na [obrázku 2-2](#), ktorý sa dodáva s kartami Orinoco, je obzvlášť šikovný). Mali by ste byť schopný získať tabuľku s prehľadom všetkých sietí v dosahu a ktoré kanály sa využívajú.



Obrázok 2-2. Nástroj Site Monitor od firmy Lucent Vám zobrazí kto používa 802.11b vo Vašej oblasti.

Ostatné (nie 802.11b) zdroje 2.4GHz rádiových emisií sa prejavujú ako šum na Vašom merači sily signálu. Ak zaznamenáte priveľa šumu na kanály, ktorý by ste chceli používať, môžete sa pokúsiť ho minimalizovať premiestnením Vášho AP, použitím väčších smerovej antény (viď. [kapitola 6](#)), alebo jednoducho prepnutím na iný kanál. Aj keď vždy chcete maximalizovať Váš prijímaný signál, je to využiteľné len ak je okolitý šum nízky.

Vzťah medzi signálom a šumom je kritickej pre každý druh komunikácie. Často je skrácovaný na SNR, čo znamená signal to noise ratio (pomer medzi signálom a šumom). Čím je číslo väčšie, o to je vyššia pravdepodobnosť, že budete mať spoľahlivú komunikáciu. (Príklady nízkych SNR si láskavo pozrite na Usenet-e.)

Samozrejme, žiadna známa technológia nedokáže určiť SNR aktuálne odosielaných, alebo prijímaných dát. Napokon predsa len musíte sami vyriešiť, ako vytiahnuť signál zo šumu, keď opustí aplikačnú vrstvu Vašej siete.

Zhrnutie: buďte dobrým susedom a rozmýšľajte nad tým čo robíte, skôr než zapnete Vaše vlastné zariadenie. Rádiové spektrum je verejný zdroj a s trochou spolupráce ho môže používať každý na to, aby dosiahol lepší prístup k sieťovým zdrojom.

2.4 Topografické mapy 101

Keď rozložíte bezdrôtové zariadenia, začnete sa pozeráť na okolité prostredie inými očami. Potrubia klimatizačných zariadení, rúrky, mikrovlnné rúry, elektrické drôty a ďalšie zdroje špinavosti začnú vyskakovať do popredia keď okolo prechádzate. Po tom čo postavíte pár uzlov, budete veľmi pravdepodobne dobre oboznámený s každým zdrojom šumu, alebo odrazu v oblasti ktorú sa pokúšate pokryť. Ale čo ak chcete rozšíriť Váš dosah na niekoľko míľový spoj bod-bod? Je lepší spôsob obhliadky vzdialeného prostredia než prejsť celú trasu spoja pešo? Možno.

USGS urobilo (a neustále ho aktualizuje) topografický prieskum každého regiónu USA. Topo (skrátene topografické) mapy z rôznych zdrojov sú dostupné v oboch podobách, na papieri, aj na CD-ROM. Ak chcete vedieť tvar terénu medzi dvoma bodmi, je USGS dobrý štartovací bod.

Papierové topo mapy sú výborný zdroj na získanie prehľadu o okolitom teréne vo Vašej oblasti. Môžete použiť pravítko na rýchle zmeranie približnej vzdialenosti medzi dvoma bodmi a určiť či sú na trase nejaké očividné prekážky. Hoci sú dobrým miestom na začatie umiestňovania dlhého spoja, topo mapy neposkytujú niektoré kritické informácie: menovite stromy a budovy. Krajina sa môže zdať vhodná na papieri, ale ak je medzi Vašimi dvoma bodmi les, alebo niekoľko vysokých budov, nie je veľká nádej na priamy spoj.

USGS poskytuje tiež DOQ (alebo Digital Orthophoto Quadrangles) zo skutočnej leteckej fotografie. Žiaľ, voľne dostupná verzia DOQ býva zastaralá (často 8 až 10 rokov) a čerstvé DOQ nie len, že sú drahé, ale často dokonca ani nie sú dostupné. Ak naozaj musíte mať najnovšie letecké fotografie Vašej oblasti, USGS Vám umožní si ich stiahnuť za 30 USD za požiadavku a 7.50-15 USD za súbor. Nepochybne zistíte, že je lacnejšie a jednoduchšie urobiť počiatočný odhad podľa topo mapy a potom jednoducho ísť von a spoj vyskúšať.

Čo je dosť zaujímavé, MapQuest (<http://www.mapquest.com/>) nedávno začal poskytovať farebné letecké fotografie (ako prídavok ku ich bežným mapám ulíc) z GlobeExplorer (<http://www.globexplorer.com/>). Aj keď je tam málo údajov o tom ako čerstvé sú ich dáta, môže to byť dobré miesto na získanie rýchleho (a zdarma) leteckého pohľadu na Vašu oblasť.

Papierové mapy môžete kúpiť hlavne v obchodoch zameraných na kempovanie, alebo ich môžete prezerať zdarma online na <http://www.topozone.com/>. Ak sa zaujímate o DOQ, choďte priamo na <http://earthexplorer.usgs.gov/>. V kapitole 6 sa pozrieme na niektoré šikovné veci, ktoré sa dajú robiť s topo mapami na CD-ROM a s Vaším GPS.

Kapitola 3. Štruktúra siete

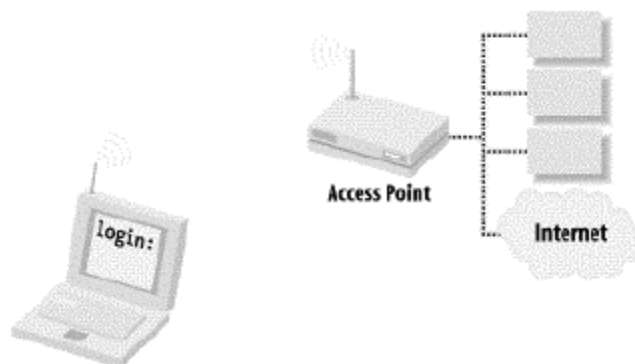
V mnohom sú 802.11b siete veľmi podobné Ethernetovým sieťam. Predpokladajme, že chcete pripojiť Vašich bezdrôtových klientov na Internet, budete chcieť poskytovať všetky obvyklé TCP/IP služby, ako sú Domain Name Service (DNS) a Dynamic Host Configuration Protocol (DHCP), ktoré robia siete tak veľmi zábavnými. Zvyšku Vašej siete sa bezdrôtoví klienti javia presne tak, ako hociktoré iné Ethernetové rozhranie a nezaobchádza sa s ňou inak než s káblovou tlačiarňou dolu v hale. Môžete smerovať (route), prepisovať (rewrite), tunelovať (tunnel), zabaliť (fold), otáčať (spindle), a/alebo znehodnocovať (mutilate) pakety od Vašich bezdrôtových klientov rovnako, ako to môžete robiť pri hocijakom inom sieťovom zariadení.

Pravdepodobne, bez ohľadu na to, koľko bezdrôtových klientov zamýšľate podporovať, asi budete potrebovať „dosiahnuť na kábel“ ak požadujete prístup na inú sieť (ako je napr. Internet). Ako nájdú pakety svoju cestu z bezuzdnej slobody vzdušných vĺn do pevne stanoveného, hyperpoprepájaného labyrintu Internetu? Táto kapitola popisuje, čo potrebujete vedieť na to, aby ste to dosiahli.

3.1 Bezdrôtová infraštruktúra: katedrála verzus bazár

Rovnako, ako pri akejkoľvek inej sieti podporujúcej rôzne fyzikálne médiá, musia existovať sieťové mosty, ktoré sú schopné vymieňať dáta medzi danými rozdielnymi typmi. Bezdrôtová brána pozostáva z rádiovkej karty a sieťovej karty (obvykle Ethernet). V prípade 802.11b, rádio zapojené do bezdrôtovej siete musí pracovať v jednom z dvoch módov: BSS, alebo IBSS.

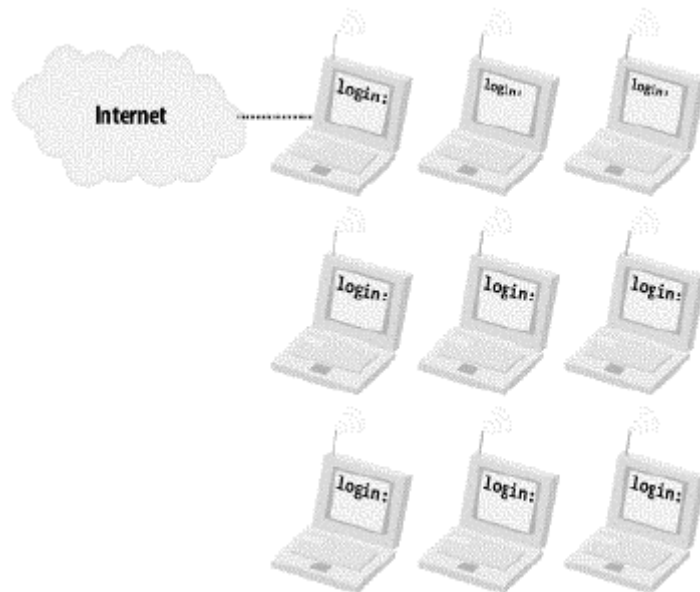
BSS znamená Basic Service Set. V tomto operačnom móde, kus hardvéru nazývaný AP poskytuje premostenie bezdrôt-na-Ethernet. Pred získaním prístupu ku káblovej sieti, musia najskôr bezdrôtoví klienti nadviazať komunikáciu s AP, ktorý je v dosahu. Potom čo AP overí bezdrôtového klienta, umožní paketom tiecť medzi klientom a pripojenou káblovou sieťou, pričom efektívne vystupuje ako pravý most 2. vrstvy (Layer 2), tak ako je to znázornené na [obrázku 3-1](#). Súvisiaci termín, ESS (alebo Extended Service Set), sa vzťahuje na fyzickú podsieť, ktorá obsahuje viac ako jedno AP. Pri tomto type usporiadania, môžu AP navzájom komunikovať a tým umožniť autentifikovaným klientom „prechádzať“ (roam) medzi nimi, pričom sú im ponechané IP informácie, aj keď menia polohu. Uvedomte si, že (keď toto píšem) nie sú žiadne AP, ktoré umožňujú roaming medzi sieťami oddelenými routerom.



Obrázok 3-1. Pri BSS (alebo ESS) móde musí klientov autentifikovať hardvér AP, predtým než budú schopný pristupovať ku káblovej sieti.

IBSS znamená Independent Basic Service Set a je často označovaný ako ad-hoc, alebo peer-to-peer (rovný s rovným) mód. Pri tomto móde nie je požadovaný žiadny AP.

Každý sieťový uzol, ktorý je v dosahu hociktorého iného, môže zahájiť komunikáciu, ak sa dohodnú na pár základných parametroch. Ak nieto z týchto seberovných má aj káblové pripojenie ku inej sieti, môže k nej poskytovať prístup. **Obrázok 3-2** znázorňuje model IBSS siete.



Obrázok 3-2. Pri IBSS móde môžu uzly v dosahu vzájomne komunikovať. Uzol, s pripojením ku inej sieti, môže poskytovať služby brány.

Uvedomte si, že 802.11b rádio musí byť nastavené na prácu v jednom z týchto režimov, ale nemôže pracovať v oboch súčasne. Oba módy podporujú WEP šifrovanie so zdieľaným kľúčom (viac o tom neskôr).

3.1.1 Hardvér prístupových bodov (AP)

AP-čka sú všeobecne považované za ideálne na pokrytie školského areálu. Tvoria jednotlivé vstupné body, ktoré sa dajú centrálnie konfigurovať. Obvykle sa dá pripojiť jedno až dve rádia na jeden AP, ktorý, teoreticky, obsluhuje stovky bezdrôtových klientov, pripojených súbežne v tom istom čase. Musia mať nastavené ESSID (Extended Service Set ID, používané pojmy sú tiež *Network Name* - meno siete, alebo *WLAN Service Area ID* - identifikátor oblasti obsluhovanej bezdrôtovou lokálnou sieťou, záleží na tom s kým sa rozprávate), je to jednoduchý reťazec, ktorý identifikuje konkrétnu bezdrôtovú sieť. Mnohé používajú klientský program na konfiguráciu a jednoduché heslo na ochranu ich sieťových nastavení.

Väčšina AP tiež poskytuje prídavné funkcie, ako sú napr.:

- Filtrovanie MAC adries. Klientské rádio pokúšajúce sa o prístup musí mať svoju MAC adresu uvedenú v internom zozname skôr než mu bude dovolené spojiť sa s daným AP.
- Uzavreté (neverejné) siete. Zvyčajne môže klient uviesť všeobecný ESSID „ANY“ platný pre pripojenie sa ku ktorejkoľvek dostupnej sieti. Pri uzavretej sieti musí klient výslovne zadať ESSID, v opačnom prípade sa nemôže pripojiť k AP.
- Externé antény.
- Nepretržité sledovanie kvality spojenia.
- Rozšírené možnosti tvorby záznamov, štatistík a hlásení o prevádzkových hodnotách.

Ďalšie rozšírené režimy zahŕňajú dynamickú správu WEP kľúčov, výmenu verejných šifrovacích kľúčov, spájanie kanálov a iné zábavné hračky. Žiaľ, tieto rozšírené režimy sú úplne špecifické pre každého výrobcu a model, nie sú zahrnuté v žiadnom pevne stanovenom štandarde a nespôlupracujú so zariadeniami iných výrobcov. Tiež by malo byť spomenuté, že keď už sa klient raz spojil s AP, nie sú žiadne ďalšie obmedzenia zo strany AP na to, ku ktorým službám môže klient pristupovať.

AP-čka sú ideálna voľba pre súkromné siete s mnohými bezdrôtovými klientmi, ktorí sú v ohraničenom fyzickom priestore, najmä na rovnakej fyzickej podsieti (ako napr.: firma, alebo vysokoškolský areál). Umožňujú vysoký stupeň kontroly, kto môže pristupovať ku sieti, ale nie sú lacné (priemerný AP ako je popísaný má cenu medzi 800 USD a 1000 USD).

Iná trieda AP je príležitostne označovaná ako *residential gateway* - brána obydľia. Apple AirPort, Orinoco RG-1000 a Linksys WAP11 sú obľúbené príklady lacnejších koncových AP. Obvykle sú oveľa lacnejšie ako ich ekvivalenty pre profesionálne použitie, s cenou medzi 200 USD a 500 USD. Mnohé majú vstavané modemy umožňujúce bezdrôtový dial-up prístup (ktorý sa môže veľmi hodiť, ak Ethernetový prístup nie je dostupný všade tam, kde sa ocitnete). Viaceré dokonca poskytujú Network Address Translation (NAT), DHCP, príp. slúžia ako mosty pre bezdrôtových klientov. Hoci nepodporujú tak veľa klientov súčasne ako špičkové AP, umožňujú lacný, jednoduchý prístup na rôzne použitie. Nastavením nie drahého AP pre premostený Ethernetový mód môžete získať vysoký stupeň kontroly nad tým, ktorí jednotliví klienti môžu využívať káblovú sieť (vid. [odstavec 7.6](#) v [kapitole 7](#)).

Napriek ich vysokej cene, AP majú svoje miesto pri budovaní bezdrôtovej komunitnej siete. Sú zvlášť dobre vhodné ako opakovače na odľahlých miestach, kvôli ich ľahkému nastavovaniu, nízkej spotrebe energie (v porovnaní so stolnými, alebo prenosnými počítačmi) a neexistencii pohyblivých častí. V [kapitole 4](#) bude detailne rozobraté ako nastaviť AP.

3.1.2 Vytvorenie siete peer-to-peer

Ak cieľom Vášho bezdrôtového projektu je umožniť verejný prístup k sieťovým službám, bude funkčnosť poskytovaná špičkovými AP takmer určite viac ako je potrebné, najmä ak zvažíme ich vysokú cenu. Našťastie, s IBSS módom, je hardvér AP-čka úplne voliteľný.

Rádia, ktoré pracujú v IBSS móde, môžu navzájom komunikovať, ak majú rovnaké nastavenia ESSID a WEP. Ako už bolo spomenuté, počítač s kartou 802.11b a ďalším sieťovým pripojením (obvykle Ethernet, alebo modem) môže slúžiť ako brána medzi dvoma sieťami. Pridajte služby DHCP a NAT a máte v skutočnosti plnohodnotnú internetovú bránu. Keďže rôzne slobodné operačné systémy dokážu poskytovať tieto služby a budú dobre fungovať s hardvérom, ktorý mnoho ľudí už nechávať ležať ladom (napr.: laptopy 486, Pentia nižšej triedy), stáva sa tento spôsob použitia čoraz populárnejšou alternatívou ku drahým AP. Ak už vlastníte počítačový hardvér, je nízka cena stavby brány naozaj lákavá (cena priemernej rádiokarty je 120 USD, alebo približne polovica AP nižšej triedy).

Čo nebolo spomenuté v rámci svojpomocne postavenej brány? Namiesto nekonečna metód riadenia prístupu, ktoré súčasné AP poskytujú, jediné dostupné riadenie prístupu je WEP. Ako sme už videli skôr, zdieľaný kľúč sám o sebe robí málo pre bezpečnosť a to rozhodne nie je vhodné v nastavení verejnej siete. Ako môžeme

poskytovať sieťový prístup a pritom zabrániť jeho zneužívaniu anonymnými bezdrôtovými klientmi? Pozri [kapitoly 5 a 7](#).

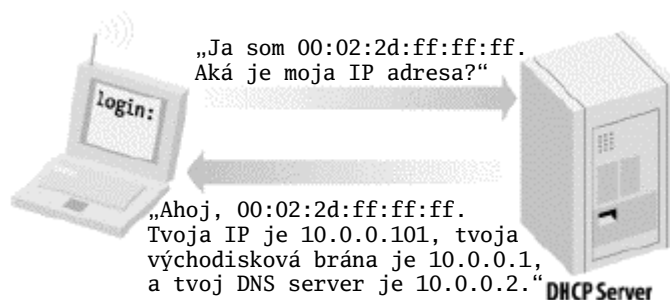
V [kapitole 5](#) vybudujeme z ničoho, od základov, bezdrôtovú bránu založenú na Linuxe. [Kapitola 7](#) popisuje spôsob rozšírenia brány tak, aby poskytovala rozdielne triedy služieb podľa toho, kto sa ku nej pripojí.

3.2 Dôležité služby

Sieť môže byť tak jednoduchá, ako je vytáčané PPP pripojenie ku ISP, alebo aj veľkolepá a vyšperkovaná ako MegaSieť medzinárodnej korporácie. Avšak každý uzol siete za niekoľko miliónov dolárov v Silicon Valley potrebuje položiť tie isté základné otázky, na ktoré musí počítač pripojený vytáčanou linkou odpovedať: *kto som, kam chcem ísť a ako sa tam dostanem odtiaľto?* Aby sa bezdrôtoví klienti mohli jednoducho pripájať k sieti, musia byť poskytované nasledujúce základné služby.

3.2.1 DHCP

Dni statických IP adries a užívateľom definovaných sieťových parametrov sú dávno za nami. Pri používaní DHCP (Dynamic Host Configuration Protocol) je možné (a dokonca triviálne) nastaviť server tak, aby odpovedal na požiadavky klientov ohľadom sieťových informácií. Obvykle DHCP server poskytuje všetky informácie, ktoré klient potrebuje na smerovanie paketov po sieti, včítane klientovej vlastnej IP adresy, východiskovej Internetovej brány a IP adries lokálnych DNS serverov. Nastavenie klienta je vo všetkých moderných operačných systémoch triviálne a v skutočnosti mimo DHCP. Kým dôkladný rozbor DHCP je mimo rozsah tejto knihy, stručný prehľad je užitočný. Typická činnosť DHCP začína keď klient zavádza operačný systém, nevediac nič o sieti ku ktorej je pripojený, okrem jeho vlastnej hardvérovej MAC adresy. Vysiela paket hovoriaci „Som tu a toto je moja MAC adresa. Aká je moja IP adresa?“. DHCP server, ktorý je v tom istom sieťovom segmente, načúva týmto požiadavkám a odpovedá: „Ahoj MAC adresa. Tu je tvoja IP adresa, a mimochodom, toto je IP adresa na ktorú smeruj odchádzajúce pakety a nejaké DNS servery sú tam. Vráť sa o chvíľu a dám Ti viac informácií.“ Klient teraz už vyzbrojený trochu vedomostí sa vydáva na šťastnú cestu. Príklad takejto komunikácie je znázornený na [obrázku 3-3](#).



Obrázok 3-3. DHCP umožňuje uzlu získať jeho sieťové nastavenia dynamicky a ľahko.

V bezdrôtovom prostredí je DHCP úplná nevyhnutnosť. Nemá veľký zmysel potulovať sa po okolí bez kábla, keď potrebujete manuálne nastaviť sieťové parametre pre každú sieť, v ktorej dosahu ste sa ocitli. Je omnoho pohodlnejšie nechať si to počítače vyriešiť po svojom (a sami sa môžete opäť venovať omnoho dôležitejším veciam, ako IRC, alebo „Quake III Arena“). Odkedy DHCP umožňuje uzlu zisťovať informácie o jeho sieti, môže byť „online“ bez akýchkoľvek predchádzajúcich vedomostí o príslušnej sieťovej štruktúre. Táto služba je príkladom požiadavky o ktorej správcovia sietí vedia už

roky: užívatelia chcú byť len pripojení, bez znalosti (či dokonca údržby) siete. Z ich pohľadu by len skrátka mala fungovať. DHCP toto kúzlo umožňuje.

Z pohľadu správcu siete nie je toto kúzlo dokonca ani veľmi ťažké uskutočniť. Pokým máte na Vašom sieťovom segmente bežiaci DHCP server môžu všetci Vaši klienti vyberať zo spoločnej množiny dostupných IP adries. Daný DHCP server sám riadi túto množinu, opätovne získava adresy, ktoré nie sú dlhšie používané a znovu ich prideluje novým klientom. V mnohých prípadoch existujúci DHCP server bezdrôtovej siete slúži bezdrôtovým užívateľom bez problémov. Na DHCP požiadavku bezdrôtového uzla pozerá ako na ktorúkoľvek inú a adekvátne reaguje. Ak Vaša káblová sieť ešte neposkytuje DHCP, alebo ak Vaša bezdrôtová brána nie je schopná L2 premostovania nemajte obavy. V [kapitole 5](#) popíšeme nastavenie *dhcpcd* servera ISC v Linuxe.

3.2.2 DNS

Nuž, nakoľko iný by bol online svet, keby sme hovorili o posielaní pošty pre *rob@208.201.239.36*, alebo keby sme boli šťastný, že sme *64.28.67.150*. DNS je živý telefónny zoznam Internetu, priradujúci mená zrozumiteľné ľuďom (ako sú [oreillynet.com](#), alebo [slashdot.org](#)), ku číslam zrozumiteľným počítačom (ako je štvorica s bodkami vyššie). Internet bez DNS je tak veľmi zábavný a pohodlný ako odkazovanie sa na ľudí podľa ich rodného čísla. Podobne ako DHCP, DNS server Vašej siete by mal byť viac než dostačujúci poskytovať služby rozoznávania mien Vaším bezdrôtovým klientom. Avšak, v závislosti na Vašich konkrétnych bezdrôtových aplikáciách môžete chcieť poskytovať ďalšie doplnujúce DNS služby. DNS server s vyrovnávacou pamäťou je vhodný na zníženie záťaže Vášho hlavného DNS servera (zvlášť ak máte veľký počet bezdrôtových klientov). Dokonca môžete chcieť zvláštny DNS pre Vaše bezdrôtové počítače, takže bezdrôtové uzly si ľahko dokážu navzájom poskytovať služby.

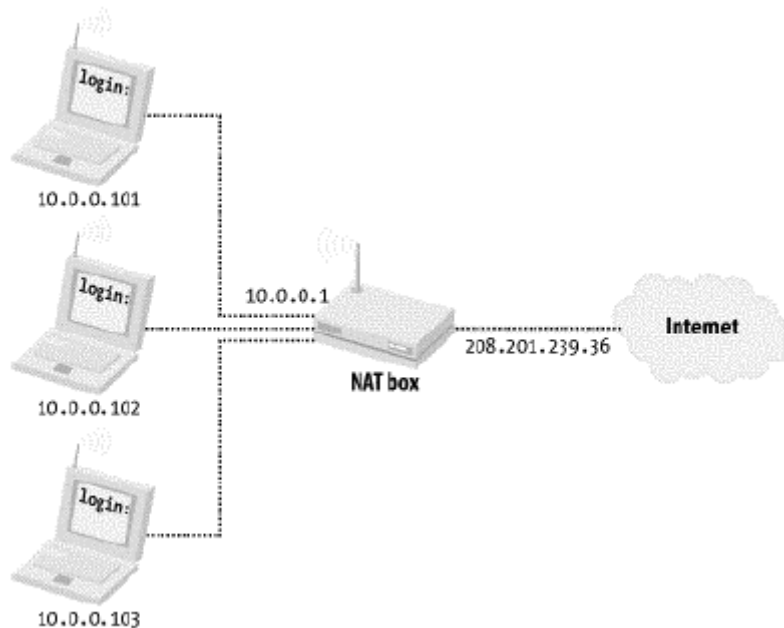
3.2.3 NAT

Aby bol každý stroj dosiahnuteľný Internetom, musí byť možné k nemu smerovať traffic. Centrálny úrad IANA (Internet Assigned Numbers Authority, <http://www.iana.org>) drží kľúče k Internetu. Tento medzinárodný orgán riadi ako sú IP adresy rozdelené do viacerých častí sveta s úsilím držať každú časť Internetu (teoreticky) dostupnú z akejkoľvek inej a zamedziť neúmyselnému opakovaniu požitíu IP adresy v inej časti sveta. Nanešťastie, kvôli nečakane obrovskej popularite Siete, to čo sa myslelo, že bude spústa adresného priestoru v čase vytvárania, sa ukázalo byť žalosťne neadekvátne v skutočnom svete. S tisíckami nových online užívateľov, ktorí pribúdajú každý deň, všeobecná zhoda je, že jednoducho už viac nie je dostatok IP adries. Mnoho ISP je čoraz viac paranoických ohľadom nedostatku obhospodarovaného priestoru a len neochotne pridelujú viac ako jednu IP adresu pre zákazníka (a v mnohých prípadoch tak už vôbec robiť nebudú, vďaka čudám DHCP).

Z toho nevyhnutne vyplýva problém: predpokladajme, že máte jednu IP adresu, pridelenú pre Vás od Vášho ISP, Vy ale chcete umožniť prístup k Internetu celej skupine strojov, vrátane Vašich bezdrôtových uzlov. Určite nechcete platiť prehnané poplatky za väčší adresný priestor, len aby ste umožnili Vášmu synovcovi byť online, keď si raz za mesiac prinesie svoj bezdrôtový prenosný počítač.

To je vec s ktorou Vám NAT môže pomôcť. Skutočné šťastie, NAT (označované v niektorých kruhoch ako maškaráda - „masquerading“) umožňuje služby dvojsmerného odosielania medzi Internetom a inou počítačovou sieťou. Počítač poskytujúci NAT má obvykle dva sieťové rozhrania. Jedno rozhranie je pripojené ku Internetu (kde používa skutočnú IP adresu) a druhé je pripojené ku internej sieti. Stroje na internej sieti

používajú niektorú z pridelených IP adries rezervovaných IANA a smerujú všetok svoj odchádzajúci prenos cez NAT box. Keď NAT box obdrží zväzok paketov pre Internet urobí si záznam odkiaľ paket prišiel. Následne prepíše paket s použitím „skutočnej“ IP adresy a odošle modifikovaný paket von k Vášmu ISP (odkiaľ ide svojou cestou cez zvyšok Internetu až dosiahne požadovaný cieľ). Keď odozva (ak je nejaká) príde späť, NAT box vyhľadá kto zadal originálnu požiadavku, prepíše prichodzí zväzok paketov a prinávrati ho pôvodnému odosielateľovi. Pokiaľ ide o zvyšok Internetu, len NAT stroj je viditeľný. Zatiaľ čo interní klienti majú pocit akoby boli pripojení priamo k Internetu. Na [obrázku 3-4](#) je znázornený príklad NAT konfigurácie.



Obrázok 3-4. Použitie NAT, niekoľko počítačov môže zdieľať jednu „reálnu“ IP adresu.

IANA rezervovala nasledujúce množiny IP adries pre súkromné použitie (ako je uvedené v RFC 1918, <http://rfc.net/rfc1918.html>):

10.0.0.0 - 10.255.255.255
 172.16.0.0 - 172.31.255.255
 192.168.0.0 - 192.168.255.255

Tieto adresy zaručene nebudú nikdy použité v Internete. Pokým budú Vaše interné stroje používať IP adresy z niektorého z týchto troch intervalov, nebudú Vaše prenášané dáta kolidovať so žiadnym iným počítačom na Internete. Ako pridaný bonus, keďže prenos rezervovaných IP adries nie je dokonca smerovaný cez Internet, získate v skutočnosti firewall pre všetky Vaše NAT-ované počítače.

NAT je šikovný, ale má aj svoju tienistú stránku. Napríklad, niektoré služby nepracujú správne s niektorými realizáciami NAT. Obzvlášť aktívne FTP spojenia zlyhávajú na niektorých NAT boxoch. Ďalšia veľká nevýhoda NAT je, že v skutočnosti robí z Internetu prostriedok len na čítanie, podobný ako televízia. Ak budete mať len odchádzajúci traffic (napr. ku web serverom) a traffic z Internetu nemôže dosiahnuť Váš stroj priamo, potom nemáte možnosť poskytovať dáta a prispievať k Sieti! To Vám nebráni používať dvojsmerné služby ako IRC a email, ale vopred Vám bráni jednoduchému fungovaniu služieb pri ktorých Internetoví používatelia sa pripájajú priamo k Vám (napr.: prevádzka Vášho web servera spoza NAT nie je jednoduchá).

Napriek týmto tienistým stránkam NAT je neoceniteľný nástroj umožňujúci davom ľudí pristupovať k Internetovým zdrojom. V [kapitole 5](#) postavíme Linuxovú bránu, ktorá bude slúžiť aj ako NAT pre Vás a bude narábať s takmer všetkými obľúbenými druhmi Internetového traffic-u (vrátane aktívneho FTP).

Samozrejme, ak máte dosť šťastia a máte tonu živého IP adresného priestoru, kľudne to dajte najavo a pridajte živé IP Vaším bezdrôtovým klientom. Prirodzene, veľa ľudí (a, v skutočnosti, ich počítače) je nepripravených na nespútaný adrenalínový ruch používania živých IP adries bez firewallu. Ale ak máte tak veľa reálnych IP na zahodenie, musíte byť veľkorysý. Netrápte sa, keď sa začnú Vaši klienti spontánne reštartovať, alebo nečakane poskytovať 0-dAy W@r3z. Toto všetko je súčasť krásneho online zážitku.

3.3 Bezpečnostné aspekty

Hoci rozdiel medzi medzi zauzdeným a bezuzdým je málo, sú významné. Napr. každý už počul pojem „black-hat packet sniffer“, chichotajúci sa sociopat sediaci na Vašom fyzickom Ethernetovom segmente, tajne zaznamenáva pakety pre svoje vlastné mrzké zámery. Môže to byť nespokojný zamestnanec, poradca so zlým vzťahom, alebo dokonca (v jednom legendárnom prípade) konkurent s prenosným počítačom, dostatkom času a veľa nervami⁴. Hoci prepínané siete, primerané pracovné prostredie a svedomitý vrátnik môžu znamenať veľa pre minimalizáciu vystavenia sa fyzickému odpočúvaniu, riziko sa zvyšuje s bezdrôtovým prístupom. Odrazu viac nikto nepotrebuje fyzickú prítomnosť na zaznamenávanie dát, načo sa unúvať pokusmi prepašovať zariadenia dovnútra, keď sa môžete nabúrať zo svojho vlastného domu, alebo kancelárie dva bloky ďalej s vysoko ziskovou anténou?

Predstava cracker-a, s bledou pokožkou, fajčiaceho cigarety v odľahlej tmavej miestnosti, to je skutočnosť, ktorú mnohí správcovia majú sklon prehliadnuť, keď plánujú výstavbu siete. Jediný dôvod pre existenciu siete je, aby spájala ľudí navzájom. Služby, ktoré sú pre ľudí zložité na používanie, jednoducho budú nevyužívané. Môžete mať najlepšiu kryptografickú metódu na svete na overovanie používateľov systémom. Dokonca môžete mať novinky z biometrickej identifikácie, najlepšie vybavenie na triedenie pliev, zabezpečenie obsahu každého jednotlivého paketu pomocou digitálneho podpisu a nezávislého overenia. Ale ak priemerný používateľ nebude môcť jednoducho skontrolovať svoj email, je to všetko nanič. Ak je cesta do pekla vydláždená dobrými zámermi, na colniciach musia určite pracovať zaničení bezpečnostní konzultanti.

Dva hlavné body pri narábaní s bezdrôtovými klientmi sú:

- Komu je dovolené pristupovať k sieťovým službám ?
- Ku ktorým službám môžu overení klienti pristupovať ?

Ako vidíte, s trochou plánovania, môžu byť tieto problémy nastolené v mnohých prípadoch skutočného sveta. V tejto kapitole si ukážeme spôsoby plánovania siete, ktorá stráži aby Vaše dáta tiekli tam kam patria, tak rýchlo a efektívne ako je to len možné.

Pozrime sa na nástroje, ktoré máme dostupné na to, aby sme mohli riadiť kto k čomu môže pristupovať.

⁴ Ako sa hovorí, významný výrobca počítačového hardvéru raz objavil nového „zamestnanca“ sediaceho v predtým neobsadenom priestore. Zjavne tam bol už tri týždne, pripojený ku podnikovej sieti a spokojne zaznamenávajúci dáta, než ho vyrušili otázkou kto je.

3.3.1 WEP

Špecifikácia 801.11b opisuje druh šifrovania nazývaný *wired equivalency privacy* - súkromie zhodné s káblom, alebo WEP. Šifrovaním paketov na MAC vrstve, len klienti ktorí poznajú „tajný kľúč“ sa môžu spojiť s AP, alebo peer-to-peer skupinou. Ktokoľvek bez kľúča, môže byť schopný vidieť sieťový prenos, ale každý paket je šifrovaný.

Špecifikácia využíva 40 bitový algoritmus zdieľaného kľúča RC4 PRNG⁵ od RSA Data Security. Mnoho kariet používajúcich 802.11b (spomeňme aspoň niektoré: Agere Orinoco, Cisco Aironet, Linksys WPC11) podporuje tento šifrovací štandard.

Hoci hardvérové šifrovanie znie ako dobrá myšlienka, realizácia podľa 802.11b má ďaleko k dokonalosti. Predovšetkým šifrovanie sa deje na linkovej vrstve, nie na aplikačnej. To znamená, že Vaša komunikácia je chránená až po bránu, ale viac už nie. Keď už raz dosiahne kábel, sú Vaše dáta poslané v čistej forme. Horšie než to je, že každý iný legitímny bezdrôtový klient, ktorý má kľúč, môže beztrešne čítať Vaše pakety, pokiaľ je kľúč zdieľaný všetkými klientmi. Sami si to môžete vyskúšať, jednoducho spustíte *tcpdump* na Vašom laptope a sledujte pakety Vášho suseda ako prelietavajú, dokonca pri aktivovanom WEP.

Niektorí výrobcovia (napr.: Agere a Cisco) zaviedli ich vlastné súkromné nadstavby na WEP, vrátane 128 bitového kľúča a dynamického riadenia kľúčov. Žiaľ, keďže nie sú definované v štandarde 802.11b, nie je zaručené, že karty od rozdielnych výrobcov, ktorí používajú tieto nadstavby, budú spolupracovať (a vo všeobecnosti nebudú).

Svojím polienkom do ohňa prispel tím kryptológov na Kalifornskej univerzite v Berkeley, ktorý odhalil slabosť v spôsobe akým je WEP realizovaný, čo robí v skutočnosti silu šifrovania nepodstatnou. Keď zoberieme všetky tieto problémy do úvahy, prečo je WEP ešte stále podporovaný výrobcami? A čo je na tom dobré pri budovaní verejnej prístupnej siete?

WEP nebol navrhnutý ako neprekonateľný bezpečnostný nástroj „zabijak“ (v skutočnosti si žiadny nemôže nárokovať takéto označenie). Jeho akronym objasní účel: súkromie zhodné s káblom. Inými slovami, cieľom WEP bolo poskytnúť nie väčšiu ochranu, než akú by ste mali, ak by ste sa fyzicky pripojili k Ethernetovej sieti. (Uvedomte si, že v nastaveniach drôteného Ethernetu nie je vôbec žiadne šifrovanie zaisťované protokolom. Na to je určené zabezpečenie aplikačnej vrstvy, viď opis tunelovania neskôr v tejto kapitole.)

Čo WEP dokáže poskytnúť je ľahký, všeobecne efektívny, odstrašujúci účinok proti neoprávnenému prístupu. Aj keď je technicky realizovateľné pre odhodlaného votrelca získať prístup, je to nie len mimo schopnosti väčšiny užívateľov, ale obvykle to nestojí za ten čas a námahu, obzvlášť keď už ste odstránili verejný prístup.

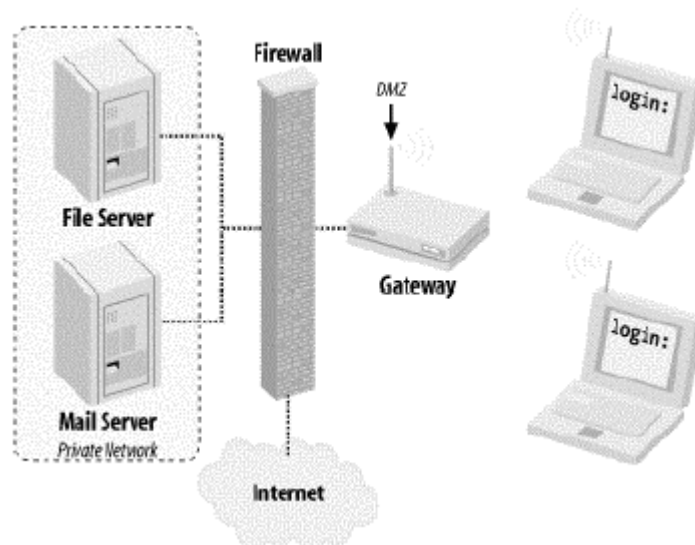
Ako si ukážeme v [kapitole 7](#), jedna z oblastí, kde je WEP obzvlášť užitočný, je na koncoch dlhého point-to-point chrbticového spoja. V tomto prípade, nežiadúci klienti by prípadne mohli znížiť výkonnosť siete veľkému počtu ľudí a WEP dokáže pomôcť nie len pri odstrašovaní zlodejov, ktorí by sa chceli pripojiť, ale aj pri presvedčaní, aby bolo viac verejných prístupových brán.

⁵ Pseudo-Random Number Generator - generátor zdanlivo náhodných čísel. Môže byť horší, ale entropia zaberá viac času.

3.3.2 Smerovanie a firewalling

Hlavným bezpečnostným aspektom pre bezdrôtový sieťový prístup je, kam ho začleniť do Vašej existujúcej siete. Bez ohľadu na Váš druh brány (AP, alebo DIY) potrebujete zvážiť, ku ktorým službám chcete, aby mali Vaši bezdrôtoví klienti prístup. Aj keď hlavným cieľom tejto knihy je popísať spôsob poskytovania verejného prístupu k sieťovým službám (vrátane prístupu na Internet) dôrazne doporučujem nastaviť Vaše bezdrôtové brány na rovnakom mieste, kde chcete nejaké verejné zdroje: v DMZ vašej siete, alebo zvonku Vášho firewall-u, v podstate. Týmto spôsobom, dokonca aj pri úplnom zlyhaní preventívnych bezpečnostných opatrení, najhoršie čo môže nejaký asociál dosiahnuť, je Internetový prístup a nie neobmedzený prístup k Vašej súkromnej internej sieti.

Táto konfigurácia, ako je zobrazené na [obrázku 3-5](#), nenecháva prakticky žiadny motív pre nikoho, aby skúšal narušiť Vašu bránu, jediná dosiahnutá vec, by mohol byť Internetový prístup. Útoky prichádzajúce z bezdrôtových rozhraní môžu jednoducho zaznamenať MAC adresu a informáciu o sile signálu. V IBSS móde je to dokonca významný strašiak. Keď potenciálny útočník potrebuje vyslať, aby vykonal útok, udáva nie len svoj unikátny identifikátor (jeho MAC adresu), ale tiež svoju fyzickú polohu!



Obrázok 3-5. Umiestnite Vašu bezdrôtovú bránu zvonku Vašej súkromnej siete!

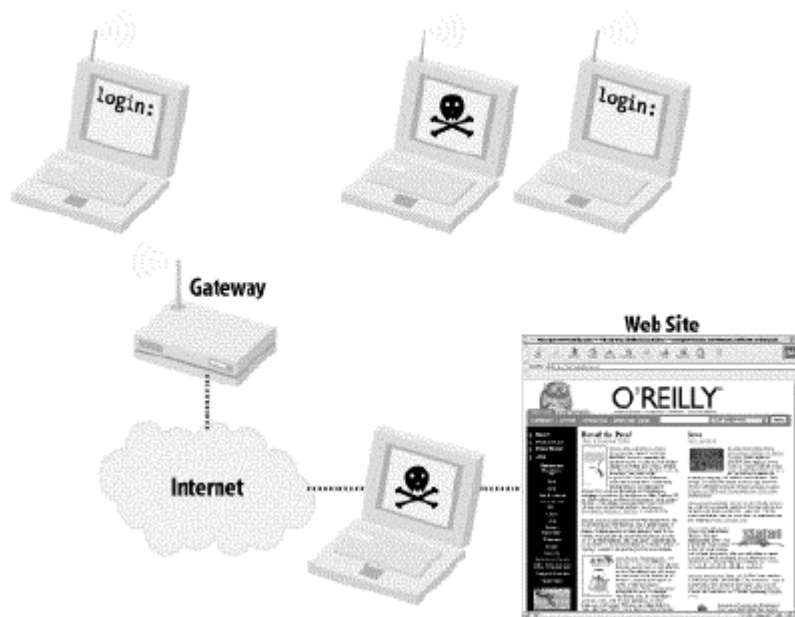
Za predpokladu, že všetky možnosti pripojenia sú umiestnené zvonka Vašej privátnej siete, čo sa stane keď sa Vy, alebo Vaši priatelia chcete pripojiť z bezdrôtovej zadnej k vnútornej sieti? Nebudú ostatní bezdrôtoví užívatelia schopní monitorovať Váš prenos a odchytiť heslá a iné citlivé informácie? [Odsek 3.3.3](#) sa zaoberá týmto potenciálnym problémom.

3.3.3 Šifrované tunely

Šifrovanie aplikačnej vrstvy je kritická technológia pri prenose informácii cez cudzie siete (ako napr. bezdrôtové spoje s verejným prístupom). Pri používaní šifrovaných tunelov, môžete zabezpečiť Vašu komunikáciu voči odpočúvaniu celou cestou, až po druhý koniec tunela.

Ak používate tunel z Vášho laptopu ku inému serveru, prípadné „black-hat“ odpočúvanie Vašej konverzácie bude mať veľmi náročnú úlohu rozlúštenia silnej kryptografie. Kým niekto nenájde lacný spôsob výstavby množstva počítačov (a snáď aj

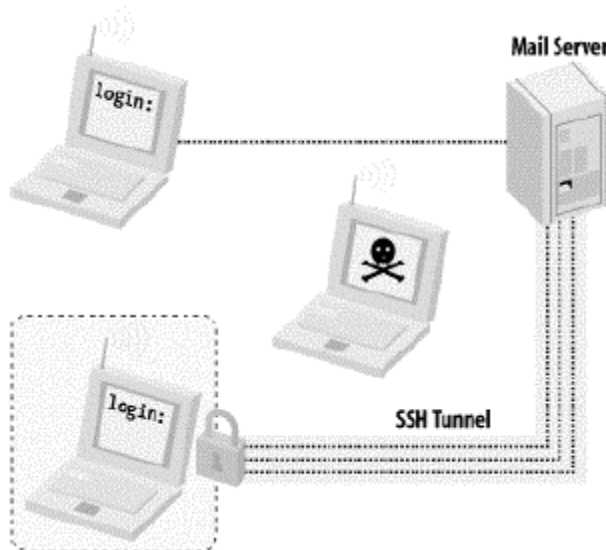
elektrárne na ich napájanie) je táto činnosť všeobecne považovaná za stratu času. Na [obrázku 3-6](#) webový server umožňujúci 128 bitové SSL pripojenie, poskytuje dostatok ochrany po celej trase, až po Váš bezdrôtový laptop. SSL poskytuje šifrovanie aplikačnej vrstvy.



Obrázok 3-6. WEP šifruje len po bránu, odhaľujúc Váš prenos ostatným bezdrôtovým klientom a všetko za káblom. Tunely chránia Váš prenos od jedného konca po druhý.

SSL je vynikajúce na ochranu webového prenosu, ale čo ostatné sieťové služby? Vezmime si typický príklad: Ste v práci, alebo doma, fúkate do bezdrôtového počítača. Chcete načítať Váš email z Vášho mailového servera pomocou POP klienta (Netscape Mail, Eudora, fetchmail, atď.). Ak sa pripojíte ku stroju priamo, Váš emailový klient pošle Vaše prihlasovacie meno a heslo v čistej forme. To znamená, že zlomyseľný jedinec niekde medzi Vami a Vaším mailovým serverom (buď kdekoľvek na Vašej bezdrôtovej sieti, alebo dokonca na kábli, ak ste oddelený ďalšou sieťou) môže počúvať a odchytiť kópiu Vašej informácie po ceste. Toto prihlasovacie meno môže byť použité nie len na získanie neoprávneného prístupu k Vášmu emailu, ale v mnohých prípadoch môže tiež udeliť účet pre príkazový interpret - shell - na Vašom mailovom serveri !

Aby ste tomu zamedzili, môžete použiť schopnosti SSH tunelovania. SSH tunel pracuje nasledovne: namiesto pripojenia sa na mail server priamo, najskôr zriadime SSH spojenie ku internej sieti, kde je mail server (v tomto prípade ku bezdrôtovej bráne). Softvér Vášho SSH klienta nastaví mechanizmus odosielania cez port, takže všetok prenos, ktorý odchádza na POP port Vášho laptopu, je zázračne odoslaný cez šifrovaný tunel a končí na POP porte mailového servera. Potom nasmerujete Vášho emailového klienta na Váš lokálny POP port a on si myslí, že hovorí so vzdialeným koncom (len teraz je celé spojenie šifrované). [Obrázok 3-7](#) zobrazuje princíp SSH tunelu pri bezdrôtovej sieti.



Obrázok 3-7. Pri správnom použití SSH tunelu, Vaša inak nie bezpečná konverzácia, ostáva súkromná.

S tunelom na správnom mieste, každý kto skúša monitorovať konverzáciu medzi Vaším laptopom a daným mailovým serverom, dostáva niečo podobné šumu na spoji. Je to dobrá myšlienka, zvyknúť si tunelovať všetko čo chcete zachovať súkromné, dokonca aj cez káblové siete. SSH tunelovanie nemusí ani zablokovať POP pripojenia. Ktorýkoľvek TCP port (napr. SMTP) môže byť jednoducho nastavený na tunel ku inému stroju s bežiacim SSH, takmer kdekoľvek na Internete. Príklad ako to dosiahnuť si ukážeme v kapitole 7. Pre úplný popis všetkých detailov tohoto veľmi prispôsobivého (a voľne dostupného) nástroja vrelo doporučujem knihu nakladateľstva O'Reilly *SSH: The Definitive Guide* od autorov Daniel J. Barrett a Richard E. Silverman.

3.4 Zhrnutie

Za účelom udržať maximum kompatibility s dostupným hardvérom klientov 802.11b a zároveň poskytovať spoľahlivý prístup na Internet, môžeme aplikovať kombináciu nie drahého hardvéru a voľne dostupného softvéru, aby sme našli prijateľnú rovnováhu medzi prístupnosťou a bezpečnosťou.

V nasledujúcich kapitolách si ukážeme ako nastaviť základný bezdrôtový prístup k Vašej existujúcej káblovej sieti. Následne vypracujeme praktický a efektívny spôsob poskytovania bezdrôtových služieb pre Vašu miestnu komunitu, za minimálnu cenu v prípade spolupodieľania sa komunity a zodpovedného prístupu jednotlivcov.

Kapitola 4. Používanie prístupových bodov - Access Point (AP)

Ako sme spomenuli v kapitole 3, AP je časť hardvéru, ktorý pripája Vašich bezdrôtových klientov ku káblovej sieti (a odtiaľ obvykle ku Internetu). Ako premostovací hardvér má prinajmenšom dva sieťové pripojenia a presúva sieťový prenos medzi nimi. Bezdrôtové rozhranie je obvykle rádio, alebo zasunutá PCMCIA bezdrôtová karta. Druhé sieťové rozhranie môže byť Ethernet, modem, alebo dokonca ďalší bezdrôtový adaptér.

Hardvér AP riadi prístup na a z oboch sietí. Na bezdrôtovej strane veľa výrobcov implementovalo metódy riadenia prístupu 802.11b (ako WEP šifrovacie kľúče, uzavretý

sieťový ESSID a filtrovanie MAC adries). Niektorí pridávajú komerčné nadstavby, aby poskytl dodatočnú bezpečnosť, napr. šifrovanie verejným kľúčom⁶. Viaceré AP tiež umožňujú kontrolovať čo môže káblová sieť poslať bezdrôtovým klientom pomocou jednoduchých firewallových pravidiel.

Navyše AP-čka tiež udržiavajú ich vlastné sieťové pripojenie, aby poskytl riadenie prístupu. To zahŕňa funkcie ako je vytáčanie a pripájanie sa k ISP na požiadanie, alebo používanie DHCP na Ethernetovom rozhraní, kvôli získaniu sieťového oprávnenia. Veľa AP dokáže poskytovať NAT a DHCP služby bezdrôtovým klientom, čím podporuje viacero bezdrôtových používateľov, zatiaľ čo požaduje iba jednu IP adresu z kábla. Niektoré podporujú priame premostovanie, umožňujúce káblovej a bezdrôtovej sieti vymieňať si dáta tak, akoby boli fyzicky spojené. Ak má AP viac rádii, môže ich premostiť spolu s káblom a vytvoriť tak veľmi pružnú a rozširiteľnú sieť.

Ďalšia dôležitá služba poskytovaná AP je schopnosť odovzdávať si klientov, keď sa potulujú medzi AP. To umožňuje užívateľom prechádzať sa napr. po areály podniku bez straty ich sieťového pripojenia. Súčasná technológia AP umožňuje len roaming medzi AP na tej istej fyzickej podsieti (t.j. AP, ktoré nie sú oddelené routerom). Nanešťastie, roaming protokol nie je špecifikovaný v 802.11b, preto každý výrobca implementoval svoj vlastný spôsob. To znamená, že odovzdávanie medzi AP od rôznych výrobcov nie je v súčasnosti možné.

V minulom roku sa prinajmenšom 20 rôznych riešení hardvéru AP dostalo na spotrebiteľský trh. Lacné modely (určené pre použitie v domácnosti, alebo malých firmách) ako Linksys WAP11 a D-Link DWL-1000AP stoja v súčasnosti cca. 200 USD. AP vyššej triedy ako Orinoco AP-1000 a Cisco Aironet 350 stoja cez 1000 USD. Obvykle drahšie zariadenie má viac vlastností, väčší dosah a celkovo stabilnejšiu prevádzku. Hoci každé AP deklaruje zhodu s 802.11b (alebo Wi-Fi⁷), nie sú všetky rovnaké. Vlastnosti navyše, ktoré prinášajú rôzne modely zahŕňujú:

- priame premostovanie ku káblovej sieti
- NAT/DHCP služby
- viacnásobné rádia (na podporu viacerých užívateľov, alebo na použitie ako repeater)
- konektor pre externú anténu
- vyšší výstupný výkon rádia (väčšina pracuje s 30mW, kým niektoré pracujú so 100mW, alebo viac).

Vo všeobecnosti, vyberte si AP vo Vašej cenovej hladine, ktoré je určené pre Vami plánovanú aplikáciu, s najvyšším možným dosahom. AP s jedným rádiom môže podporovať niekoľko užívateľov súbežne, a ako uvidíme v [kapitole 6](#), pridanie AP do Vašej siete je možno vhodnejšie, než pridávanie viac-ziskových antén, či zosilňovačov, ku existujúcim AP.

4.1 AP upozornenia

Jedna vlastnosť, po ktorej je veľký dopyt (medzi užívateľmi pokúšajúcimi sa prekonať vzdialenosť), je schopnosť premostenia vzduchom, ku inému AP. Údajne Intel 2011 dokáže robiť premostenie AP ku AP (rovnako Linksys WAP11 po aktualizácii firmvéru). Ale správy z prevádzky vyzerajú, akoby naznačovali prinajmenšom nestabilnú

6 Nanešťastie, ako je obvyklé v prípade komerčných nadstavieb, tieto služby môžu byť použité len ak všetci Vaši sieťoví klienti používajú hardvér od rovnakého výrobcu.

7 Wi-Fi je marketingovo zaujímavý názov, vybraný organizáciou WECA (the Wireless Ethernet Compatibility Alliance), ktorým sa preukazuje zhoda zariadenia s 802.11b. Pozri <http://www.weca.net/> pre viac podrobností.

prevádzku. Obvykle AP nekomunikujú navzájom vzduchom, sú navrhnuté na komunikáciu s klientskými kartami. Preto na spojenie bod-bod dlhšej vzdialenosti potrebujete buď použiť klientský PC router na komunikáciu s AP, alebo použiť dva routery v IBSS móde (bez AP). Pozri informácie v [odseku 7.1](#) v [kapitole 7](#) ak sa zaujímate o spoje bod-bod na dlhú vzdialenosť. V čase keď sa bude tlačiť táto kniha, by výrobcovia mali mať ich firmvér v lepšom stave (dúfajme).

Tiež by ste mali starostlivo zvážiť, ako začleniť AP do Vašej existujúcej káblovej siete. Dokonca aj s WEP šifrovaním a ďalšími spôsobmi kontroly prístupu v činnosti je bezpečnosť AP ďaleko od dokonalosti. Pretože AP je, ako inak, v dosahu všetkých bezdrôtových užívateľov, môže každý užívateľ spojený s Vaším AP, vidieť traffic každého ďalšieho užívateľa. Okrem dát chránených iným spôsobom a to šifrovaním na aplikačnej vrstve, sú všetky emaily, web traffic a ďalšie dáta ľahko čitateľné hocikým, kto má spustený nástroj na analýzu protokolu, ako sú *tcpdump* alebo *ethereal*. Ako sme videli v [kapitole 3](#), spoliehanie sa na samotný WEP, že zabráni ľuďom vstúpiť do Vašej siete, nemusí byť dostatočná ochrana proti cielenému odpočúvaniu.

Pokiaľ ide o budovanie komunitnej siete, AP poskytujú jednu absolútne rozhodujúcu službu: je to ľahký, štandardný a lacný nástroj na pripojenie bezdrôtových zariadení ku káblovej sieti. Keď raz bezdrôtový traffic dosiahne kábel, môže byť smerovaný a manipulovaný rovnako, ako ktorýkoľvek iný sieťový traffic, ale najskôr sa naň musí dostať.

Bezdrôtové AP, ktoré sú dnes na trhu boli navrhnuté na pripojenie malej skupiny dôveryhodných ľudí ku káblovej sieti a vymknutie každého iného. Metódy riadenia prístupu implementované v AP odrážajú túto filozofiu a ak to je spôsob ako zamýšľate využívať dané zariadenie, malo by Vám slúžiť veľmi dobre. Napríklad si predstavme, že chcete zdieľať bezdrôtový sieťový prístup s Vaším susedom, ale nie so zvyškom bloku. Mohli by ste sa rozhodnúť pre vzájomný súkromný WEP kľúč a súkromný ESSID a držať to v tajnosti medzi Vami. Pretože Vy pravdepodobne dôverujete Vášmu susedovi, mohlo by toto usporiadanie fungovať vám obojom. Dokonca by ste mohli zostaviť zoznam všetkých rádii, ktoré máte v úmysle používať v sieti a limitovať AP, aby sa umožnil pripojiť len im. To si vyžaduje viac administratívnej réžie, keďže niekto z Vás by mal robiť zmeny na AP vždy, keď chcete pridať ďalšie zariadenie, ale umožní to v ďalšom limitovať kto môže pristupovať k Vašej bezdrôtovej sieti.

Zatiaľ čo zdieľaný tajný WEP kľúč a statická tabuľka hardvérových MAC adries môže byť praktická pre domácnosť, alebo malú kanceláriu, tieto metódy riadenia prístupu sú nepredstaviteľné pri nastavení verejného prístupu. Ak máte v úmysle poskytovať sieťové služby pre Vašu lokalitu, tento spôsob riadenia prístupu „všetko, alebo nič“ je nepoužiteľný. Ako uvidíme v [kapitole 7](#), môže byť omnoho vhodnejšie nechať každého aby sa pripojil k Vášmu AP a použil iné spôsoby identifikácie užívateľov a udelenia ďalšieho prístupu. Tieto služby sú umiestnené za samotným AP, menovite na routeri, ku ktorému je AP priamo pripojené (viď diskusia o portále v [kapitole 7](#)). Také usporiadanie vyžaduje o trochu viac zariadení a úsilia na začiatok, ale môže podporovať stovky ľudí naprieč množstvom spolupracujúcich bezdrôtových uzlov s veľmi malou administratívnou réžiou.

Skôr než dostaneme priveľkú chuť, musíme pochopiť ako nakonfigurovať AP. Pozrime sa ako nastaviť veľmi populárny AP - Apple AirPort.

4.2 Apple AirPort základňa

Mac AirPort je úžasne obľúbený AP. Vyzerá ako hladká, retro-futuristická rekvizita z filmu „War of the Worlds“ a je ľahko prenosný a veľmi kompaktný. Hoci je navrhnutý pre použitie s platformou Mac, veľmi dobre funguje ako AP na všeobecné použitie (a dokonca ani nepotrebuje Mac, aby ste ho nakonfigurovali, viď nasledujúci odsek). V čase keď to píšem, AirPort predávajú za 299 USD. Čo Vám môže poskytnúť?

- priame Ethernet premostenie
- DHCP/NAT
- 56K modemový port
- užívateľom definovateľný ESSID
- podpora roaming-u
- filtrovanie MAC adries
- WEP šifrovanie

Čo Vám neposkytne? Má len jedno rádio (konkrétne osadená karta Orinoco Silver) a žiadny konektor pre externú anténu. Ale to nie je veľký problém, pretože interná Silver karta samotná má externý konektor. Príklady ako pridať Vašu vlastnú anténu pozri na <http://homepage.mac.com/hotapplepi/airport/>, alebo <http://www.wvc.edu/~froho/Airport/Airport.html>.

Po vybalení sa AirPort pokúsi získať DHCP oprávnenie z Ethernetu a začne obsluhovať NAT a DHCP bezdrôtovo, bez hesla. Áno, jednoducho zapojíte Vašu novú hračku do Vašej LAN, a odstránili ste všetku ťažkú prácu, ktorá sa presunula na nastavenie Vášho firewallu. Každý kto je na doslech má neobmedzený bezdrôtový prístup ku sieti do ktorej ste AP zapojili.

Hoci to môže byť pohodlné ako predvolené nastavenie (povedzme na konferencii, alebo inej sieti s verejným prístupom), pravdepodobne to nie je to čo chcete. Aby ste zmenili prednastavenia, budete potrebovať konfiguračný softvér.

4.2.1 Ovládací softvér prístupového bodu

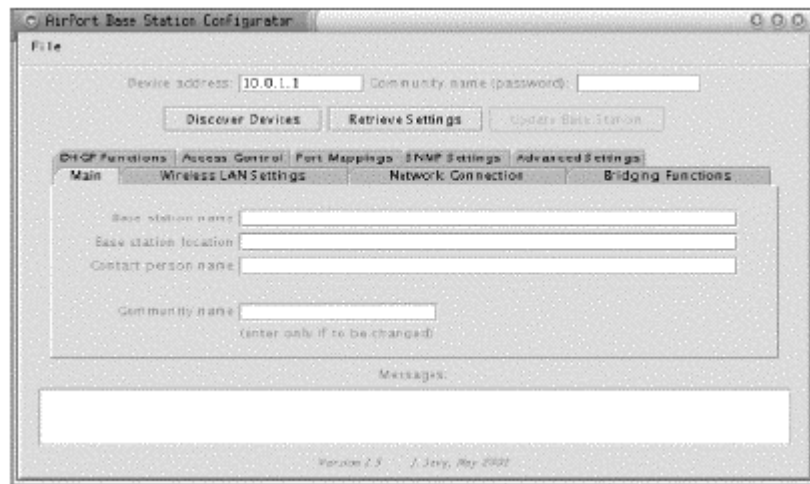
Ak vlastníte Mac, máte šťastie. Správcovská pomôcka dodávaná s AirPort-om je vynikajúca (aj keď len pre Mac OS 9 a vyšší). Apple sa pousiloval urobiť celý AirPort systém ľahký na ovládanie, dokonca aj pre začiatočníkov. Ak nevlastníte Mac, máte pár možností. Je známe, že vnútornosti AirPort-u sú vlastne rovnaké ako má Orinoco RG-1000 (predtým Lucent Residential Gateway). To znamená, že RG konfiguračná utilita pre Linux (nazvaná *cliproxy*) pracuje tiež s AirPort-om. Kópiu utility *cliproxy* od Lucentu môžete získať na <http://www.wavelan.com/>.

Jon Sevy si dal obsiahlu prácu s AirPort-om a vydal Java klient s otvoreným kódom, ktorý konfiguruje Airport a RG-1000. Kópiu môžete získať na <http://edge.mcs.drexel.edu/GICL/people/sevy/airport/>. Taktiež skompiloval obrovské množstvo informácií o vnútornom chode AirPort-u a má mnoho zdrojov online na uvedenej stránke. Keďže jeho pomôcka má otvorený kód a je viac-platformová (a pracuje veľmi dobre) budeme ju používať v nasledujúcich príkladoch.

Aby ste mohli používať Java Configurator, musíte mať nainštalovaný Java Runtime Environment. Stiahnuť ho môžete z <http://java.sun.com/>, ak ho ešte nemáte. Spustiť danú utilitu môžete v Linuxe nasledujúco:

```
$ java -jar AirportBaseStationConfig.jar &
```

Alebo môžete utility spustiť dvojklikom na ikone AirportBaseStationConfig vo Windows. Na [obrázku 4-1](#) je príklad konfiguratora.



Obrázok 4-1. AirPort Java Configurator

AirPort môže byť konfigurovaný cez Ethernet, alebo bezdrôtovo. Keď sa otvorí okno aplikácie, môžete kliknúť na tlačidlo *Discover Devices*, aby ste automaticky vyhľadali všetky AP na Vašej sieti. Keď nájdete IP adresu AP-čka, ktoré chcete konfigurovať, zadajte ju do políčka *Device address* a zadajte heslo do políčka *Community name*. Ak si nie ste istý IP adresou, alebo heslom, AirPort použije prednastavené heslo - *public* a IP adresu *10.0.1.1* na bezdrôtovom rozhraní (takto získa káblovú IP adresu prostredníctvom DHCP, použi *Discover Devices* na jej nájdenie, ak ho konfiguruje cez Ethernet). Keď už ste zadali správne údaje, kliknite na tlačítko *Retrieve Settings*.

Úplne prvá vec, ktorú by ste mali zmeniť, je *Community name* na prvom paneli. V opačnom prípade, ktokoľvek môže prekonfigurovať Váš AirPort, použitím prednastaveného *public*! Keď už ste tam, môžete nastaviť názov AirPort-u (ktorý sa zobrazí pri skenovaní siete) a taktiež umiestnenie a kontaktné informácie, ak chcete. Tieto rubriky sú úplne voliteľné a nemajú žiaden vplyv na činnosť.

Tiež by ste mali zvoliť *Network name*, pod záložkou *Wireless LAN Settings*. Tiež je to nazývané ESSID a stotožňuje to Vašu sieť s klientmi v dosahu. Ak prevádzkujete „uzavretú“ sieť, vyžaduje to, aby ho vopred poznal každý počítač, pokúšajúci sa pripojiť, tak ako je to popísané v nasledujúcom odseku.

4.2.2 Lokálny prístup k LAN

Ako bolo skôr spomenuté, prednastavená konfigurácia AirPort štandardne umožňuje LAN prístup. Ak používate DSL, káblový modem, alebo ste inštalovali AirPort na existujúcu Ethernetovú sieť, tak je to to čo chcete použiť. V Java konfiguratore sa pozrite na záložku *Network Connection* a zaškrtnite rádio tlačítko *Connect to network through Ethernet port*.

Tu môžete nastaviť, či sa bude konfigurovať IP adresa AirPort-u pomocou DHCP, zadáním IP ručne, alebo použitím PPPoE. Pravdepodobne budete chcieť použiť DHCP, s výnimkou ak Váš ISP požaduje ručné zadávanie IP adresy, alebo PPPoE.

4.2.3 Konfigurovanie vytáčania – dial-up

V záložke *Network Connection* je tiež rádio tlačítko nazvané *Connect to network through modem*. Použite túto voľbu ak Vaše jediné sieťové pripojenie je vytáčané. Áno, je to veľmi pomalé, ale aspoň ste bezdrôtový. Všimnite si, že voľby dial-up a Ethernet sa vylučujú a nemôžu byť použité súčasne.

Keď zaškrtnete *Connect to network through modem*, budete vyzvaný zadať telefónne číslo, inicializačný relazec modemu a ďalšie rubriky spojené s dial-up. Uistite sa, že *Automatic dialing* je zaškrtnutý, takže vytočí telefonické spojenie, keď začnete používať AirPort. Kliknite na tlačítko *Username/Password/Login Script* a zadajte Vaše prihlasovacie údaje. Ak to potrebujete, môžete na tejto obrazovke definovať vlastný prihlasovací skript. Prednastavený skript mi fungoval spoľahlivo s niekoľkými rôznymi ISP.

Keď už je raz AirPort nakonfigurovaný pre dial-up, bude vytáčať telefonické spojenie a pripájať vždy, keď zaregistruje Internetovú premávku na bezdrôtovom porte. Skrátka začnete používať Vašu bezdrôtovú kartu ako obvykle a po počiatočnom oneskorení (kým sa vytočí telefonické spojenie) ste online.

4.2.4 NAT a DHCP

Štandardne, AirPort vystupuje ako obidva, NAT aj DHCP server, pre Vašich bezdrôtových klientov⁸. Služba DHCP je riadená záložkou *DHCP Functions*. Aby ste spustili DHCP, zaškrtnite bunku *Provide DHCP address delivery to wireless hosts*. Môžete zadať rozsah IP adries, ktoré sa budú používať, štandardne AirPort ponúkne adresy medzi 10.0.1.2 a 10.0.1.50. Môžete tu tiež nastaviť dobu platnosti. Táto doba označuje dobu životnosti (v sekundách) vydanéj IP adresy. Po vypršaní tejto doby sa klient znova pripojí ku DHCP a požiada o inú adresu. Prednastavená 0 (alebo bez limitu) je pravdepodobne vyhovujúca pre väčšinu inštalácií, ale môžete chcieť nastaviť kratšiu dobu, ak máte veľké množstvo klientov pokúšajúcich sa pripojiť k Vášmu AirPort-u.

Ak nemáte iný DHCP server vo Vašej sieti, AirPort dokáže rovnako poskytovať službu Vaším káblovým klientom. Zaškrtnite bunku *Distribute addresses on Ethernet port, too*, ak chcete túto funkčnosť.



Zaškrtnite túto bunku len ak nemáte iný DHCP server vo Vašej sieti! Viac ako jeden DHCP server na tej istej podsieti je zlá vec a obráti hnev správcu systému na Vás. Sledovanie dvoch DHCP serverov, súperiacich kto prideli IP adresu, môže byť zábavné vo Vašom voľnom čase, ale môže spôsobiť pád celej siete a nechá Vás žasnúť, kam sa podela Vaša snaha. Mimochodom, kvôli čomu ste pripájali nepovolené zariadenia k firemnej sieti?

Ak máte viac ako jeden AirPort na tej istej káblovej sieti, presvedčte sa, že ste aktivovali DHCP pre kábel len na jednom z nich a opäť, len ak ešte nemáte DHCP server.

NAT je veľmi užitočný ak nemáte veľa IP adries na pridelovanie (a dnes len málo ľudí má). NAT tiež poskytuje Vaším bezdrôtovým klientom určitú ochranu zo strany káblovej siete, plní úlohu účinného jednocestného firewallu (úplný popis NAT a DHCP pozri v [kapitole 3](#)). V konfigurátore sa NAT nastavuje v záložke *Bridging Function*. Aby ste

⁸ Pre tých, ktorí začali čítať odtiaľto, NAT a DHCP znamená Network Address Translation a Dynamic Host Configuration Protocol. Viac informácií možno nájsť v [kapitole 3](#).

aktivovali NAT, kliknite na rádiové tlačítko *Provide network address translation (NAT)*. Môžete buď zadať Vašu súkromnú adresu a masku siete, alebo ponechať prednastavené (10.0.1.1 / 255.255.255.0).

4.2.5 Premosťovanie - Bridging

Veľká nevýhoda prevádzkovania NAT na Vašich bezdrôtových počítačoch je, že sa stanú menej prístupné pre káblové počítače. Zatiaľ čo bezdrôtový užívateľ sa môže spojiť s ktorýmkoľvek strojom na kábli, spojenie opačným smerom cez NAT je obtiažné (AirPort na to poskytuje nejakú základnú podporu, umožnením statického mapovania portu, ale nie je to vyhovujúce). Napr. ak beží Windows-ovský klient bezdrôtovo, v okne Počítače v sieti sa zobrazia len ostatné bezdrôtové počítače a žiadne káblové počítače, pretože NAT účinne schová vysielaný traffic (na ktorý sa spolieha Windows SMB protocol). Ak už máte DHCP server na Vašej káblvej sieti a používate súkromné adresy, NAT a DHCP funkcie AirPort-u sú prebytočné.

Radšej než zdvojsť úsilie a robiť život ťažkým, môžete vypnúť NAT a DHCP a vytvoriť premostenie ku káblu. Vypnite DHCP pod *DHCP Functions* (ako sme videli skôr) a zaškrtnite *Act as transparent bridge (no NAT)* v záložke *Bridging Functions*. Keď AirPort pracuje v tomto móde, je všetok traffic určený pre Vašich bezdrôtových klientov, ktorý sa udeje na kábli, odvysielaný bezdrôtovo a opačne. Vráťane vysielaného trafficu (ako sú DHCP požiadavky a SMB informačný traffic). To spôsobí, keď si odmyslíme bezdrôtovú autentifikáciu, že sa zdá, akoby bol AirPort neviditeľným pre zvyšok Vašej siete.

Keď už je raz premostenie aktivované, môže byť pre Vás obtiažné dostať jednotku späť do NAT módu. Aj keď sa zdá, že Java konfiguratör (alebo Mac AirPort admin utilita) nereaguje, kým je v premostovacom móde, je pár spôsobov ako ho prestaviť späť.

Ak máte Mac, môžete vykonať ručný reset. Stlačte drobné tlačítko na spodku AirPort-u s kancelárskou sponkou na približne dve sekundy. Stredná zelená kontrolka na vrchu sa zmení na jantárovú. Pripojte Ethernetový port na Vašom AirPort-e na Váš Mac a spustíte utilitu admin. Softvér by Vám mal umožniť nastaviť prednastavené hodnoty. Máte päť minút na to, aby ste to urobili, než sa jantárová kontrolka zmení na zelenú a vráti do premostovacieho módu.

Ak používate Linux, môžete jednoducho, online, prestaviť AirPort späť, použitím Lucentovskej utility *cliproxy*, bez potreby tvrdého resetu. Spustíte nasledujúce príkazy z Linuxového stroja (buď cez kábel, alebo po pripojení bezdrôtovo):

```
$ cliproxy
[ORiNOCO]> show accesspoints
Searching...
```

Hostname	Eth Address	IP Address	Description
NoCat	0030.42fa.cade	192.168.0.5	Base Station V3.64

```
[ORiNOCO]> configure remote 192.168.0.5 public
Config loaded from 192.168.0.5
```

```
NoCat> configure terminal
```

```
NoCat(config)> no service bridging
```

```

NoCat(config)> service napt
NoCat(config)> service dhcp-server
NoCat(config)> done
NoCat> write remote 192.169.0.5 public
NoCat> exit

```

Samozrejme nahraďte Vaše heslo za *public* a Vašu IP adresu za predchádzajúci vzor. Po tomto by sa AirPort mal rebootovať s aktivovaným NAT a DHCP a vypnutým premostovaním.

Ak používate Windows a potrebujete resetovať AirPort v premostovacom móde, doporučujem Vám nájsť kamaráta, ktorý má Mac, alebo Linux. Môžete byť schopný dostať veci späť do normálu vykonaním tvrdého resetu (podržaním stlačeného tlačidla reset pomocou kancelárskej sponky na 30 sekúnd pri zapínaní jednotky), ale mne sa to nikdy nepodarilo. Predchádzajúce dva spôsoby, použitie tvrdého resetu s Mac, alebo Linuxová utilita *cliproxy*, pracovali v minulosti veľmi spoľahlivo. Len z tohto dôvodu mám kópiu *cliproxy* stále poruke.

4.2.6 WEP, MAC filtrovanie a uzavretie siete

Ak skutočne chcete uzamknúť Vašu sieť v mieste AP, máte k dispozícii nasledujúce nástroje: WEP šifrovanie, filtrovanie MAC adries (sériové číslo rádiovkej karty) a používanie uzavretej siete. Tieto tri služby sú úplne nezávislé, preto nemusíte napr. používať MAC filtrovanie spolu s uzavretou sieťou. Kombinácia všetkých týchto možností nemusí urobiť Vašu sieť úplne bezpečnou pred cieľavedomými podliakmi, ale aspoň odradí väčšinu potenciálnych útočníkov.

Pre nastavenie WEP kľúčov kliknite na záložku *Wireless LAN Settings* a zadajte kľúče do príslušných rubrik. Tiež zaškrtnite *Use encryption* a vymažte zaškrtnutie *Allow unencrypted data*, keďže požadujete WEP na Vašej sieti. Kópiu tohto kľúča dajte každému Vášmu bezdrôtovému klientovi.

S aktivovaným MAC filtrovaním, si AirPort udržiava internú tabuľku MAC adries, ktorým je dovolené používať AirPort. Kliknite na záložku *Access Control* a zadajte potrebný počet MAC adries. Len rádiám, ktoré používajú niektorú z MAC adries v zozname, bude povolené spojiť sa s AirPort-om. MAC adresa rádiovkej karty by mala byť vytlačená na jej zadnej strane (MAC adresa pozostáva zo šestice hexadecimálnych čísel v tvare *12:34:56:ab:cd:ef*).

Uzavretá sieť spôsobí, že AirPort odmietne spojenia z rádií, ktoré nemajú explicitne uvedený ESSID, t.j. klienti s prázdny ESSID, alebo tí ktorí majú nastavené ANY. Aby ste vytvorili uzavretú sieť, zaškrtnite políčko *Closed network* pod *Wireless LAN Settings*.

Uvedomte si, že bez šifrovania je všetok traffic prenášaný v zrozumiteľnej forme, takže ktokoľvek v dosahu môže prípadne čítať a zneužiť citlivé informácie (ako sú ESSID a platné MAC adresy). Dokonca aj s WEP môže každý legitímny užívateľ vidieť tento traffic. Ak potrebujete užívateľom obmedziť prístup neskôr, je potrebné zmeniť WEP kľúč na každom bezdrôtovom klientovi. Avšak, pri malej skupine dôveryhodných užívateľov, by používanie týchto metód kontroly prístupu malo odstrašiť všetkých, okrem najviac odhodlaných „black-hat“, bezo sporu.

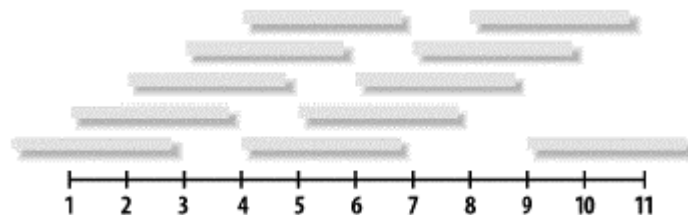
4.2.7 Roaming

Bezdrôtový roaming môže byť veľmi šikovný, ak je Vaša sieť navrhnutá tak, že ho môžete podporovať. Aby bolo možné vyhovieť požiadavke na roaming, musia byť všetky Vaše AP od rovnakého výrobcu, musia byť umiestnené na tej istej fyzickej káblovej podsieti (t.j. na tej istej sieťovej IP, bez potreby routerov) a musia mať rovnaké *Network name* (ESSID).

Čo sa týka AirPort-u, je roaming automaticky aktivovaný, ak sú všetky tieto podmienky splnené. Uistite sa, že všetky Vaše AirPort-y majú uvedené presne rovnaké *Network name* pod *Wireless LAN Settings*. Ak z nejakej príčiny chcete vypnúť roaming, jednoducho zadajte pre každý AirPort iný ESSID.

4.2.8 Odstup kanálov

Podľa špecifikácie 802.11b (v USA) je 2.4GHz spektrum rozdelené na 11 prekrývajúcich sa kanálov. V ideálnom prípade, keď pridávate AP do Vašej siete chcete dosiahnuť, aby sa oblasti (alebo bunky) pokryté Vaším signálom mierne prekrývali, takže nie sú žiadne medzery v pokrytí. Všade, kde je to možné, mali by ste dodržať odstup minimálne 25MHz (alebo 5 kanálov) medzi susediacimi bunkami, tak ako je to znázornené na [obrázku 4-2](#). V opačnom prípade môže traffic AP nachádzajúcich sa blízko seba interferovať, čo spôsobí zníženie výkonnosti.



Obrázok 4-2. Kanály musia mať odstup minimálne 25MHz, aby sa predišlo prekrývaniu a nožnej interferencii.

Napríklad môžete používať kanály 1, 6 a 11 šachovnicovo usporiadané tak, aby ste úplne pokryli danú oblasť, bez akéhokoľvek prekrývania sa frekvencií. Samozrejme, každý kto používa 802.11b sa pokúša urobiť to isté a zrejme bude používať niektorý z týchto kanálov. Obzvlášť v preľudnených oblastiach dokonalý 25MHz odstup nebude možný. Ak je to nutné, môžete sa priblížiť až na odstup dvoch, alebo troch kanálov, ale nikdy neskúšajte prevádzkovať dve susediace siete na tom istom kanály (zo začiatku sa môže zdať všetko v poriadku, ale keď stúpne zaťaženie, sieť spadne).

Aby ste zistili, ktoré kanály používajú Vaši susedia, pozrite sa na merač sily signálu, alebo iný nástroj, ktorý je dodávaný s Vašou bezdrôtovou kartou (napr. karta Orinoco je dodávaná s výbornou utilitou *Site Map*). Môžete sa tiež poohliadnuť po *NetStumbler*-i, čo je výborný pátrací nástroj pre MS Windows. Zdarma ho môžete získať na <http://www.netstumbler.com/>.

Kapitola 5. Peer-to-Peer (Ad-Hoc) sieť

Pri tradičnej káblovej sieti je pre jej existenciu dôležité, aby mal expert vysoký stupeň kontroly nad tým, čo sa deje v jeho kábloch. Cez hraničné firewally, proxy, filtre paketov a inteligentné smerovanie je napokon obsah siete, dostupný jednotlivým uzlom, spracovaný takmer nekonečným počtom stupňov.

Pravidlá sa celkom zmenia, keď odoberieme káble. Každý s 802.11b kartou môže skutočne generovať akýkoľvek druh paketov ktorý chce a posilať ich von komukoľvek v dosahu. Pokým budú uzly súhlasiť so spoločným spôsobom komunikácie, ľubovoľný počet peer-to-peer sietí môže byť vytvorený na výmenu dát, spôsobom ktorý znemožňuje jednej osobe zaviesť nejaký druh obmedzení na prenos údajov.

IBSS mód je jeden z najliberálnejších aspektov protokolu 802.11b. V skutočnosti robí drahý hardvér AP úplne voliteľným, miesto toho sa spolieha, že každý uzol siete sa postará o svoju vlastnú komunikáciu. Namiesto centralizovaného modelu, kedy všetci klienti musia byť vo vnútri okruhu AP, aby sa mohli pripojiť, IBSS umožňuje každému uzlu komunikovať s hociktorým iným čo je na dosluch. Ak sa jeden z týchto uzlov stane bránou k Internetu, môže nie len poskytovať služby podobné AP, ale aj také veci ako smerovanie paketov, regulovať šírku pásma, slúžiť ako firewall, atď.

Zatiaľ čo IBSS sa vzťahuje na špecifický mód 802.11b operácií, narazíte tiež na pár iných podobných (a používaných) výrazov: ad-hoc a peer-to-peer. Niekoľko výrobcov implementovalo ich vlastný „bez AP“ spôsob činnosti, ktorý ojedinele poskytuje niektoré zaujímavé funkcie, ale nie je v súlade so štandardom IEEE a bude fungovať len na ich vlastnom hardvéri. Tieto komerčné módy sú v dokumentácii k produktom nazývané ako ad-hoc, alebo peer-to-peer. Karty, ktoré rešpektujú ustanovenia 802.11b, môžu podporovať tieto prídavné komerčné módy, avšak musia tiež podporovať pravú IBSS komunikáciu.

A aby to nebolo také jednoduché, Linuxový balík bezdrôtových nástrojov nazýva ľubovoľný nie-AP mód ad-hoc a umožní Vám vybrať si ktorý má používať (IBSS, alebo komerčný) pomocou systémového volania. V záujme maximálnej kompatibility sa v ďalšej časti knihy budeme zaoberať len pravým IBSS módom, a budeme používať termíny IBSS, ad-hoc a peer-to-peer ako ekvivalentné (ak nie je uvedené inak).

5.1 Stavba bezdrôtovej brány pod Linuxom

Pre Linuxový stroj sa bezdrôtová karta javí jednoducho ako ďalšie Ethernetové zariadenie. Ovládač pre bezdrôtové zariadenia, ktorý je v jadre, vytvorí sieťové zariadenie (napr. *eth0*), ktoré môže robiť všetky veci ako hociktoré iné sieťové zariadenie. Zvyšok systému nevie vôbec nič o tom, že komunikácia prebieha cez rádio. Ak ste už niekedy stavali firewall pod Linuxom, veľa z tohto odseku sa Vám bude zdať známe.

Ak ste ešte firewall pod Linuxom nepostavili, vrele Vám doporučujem jeden postaviť na zastaranom Ethernete, aby ste sa s tým oboznámili. Kniha *Building Internet Firewalls* z vydavateľstva O'Reilly popisuje špecifické problémy omnoho podrobnejšie, než je na to daný priestor v tejto knihe. Ďalší výborný dokument je HOWTO (ako na to) pre Firewall a Proxy server na <http://www.linuxdoc.org/HOWTO/Firewall-HOWTO.html>.

5.1.1 Hardvér

Veľa 802.11b kariet, ktoré sú dnes na trhu, sú PCMCIA zariadenia. Z pohľadu vývoja a výroby je to výborný nápad, pretože to zjednodušuje výrobnú linku a pomáha

udržať nízku cenu. V čase písania tejto knihy stoja bezdrôtové karty niekde medzi 75–200 USD, s priemerom okolo 120 USD. Nenechajte sa zmiasť ich malými rozmermi, tieto drobné karty sú schopné, s príslušnou anténou, posilať signál na niekoľko míľ.

Samozrejme, aby sme nastavili stroj ako bezdrôtovú bránu, potrebujeme počítač s minimálne jedným PCMCIA slotom. Hoci obvykle počítače, ktoré podporujú PCMCIA, sú laptopy, montážny blok pre stolný, alebo stojanový počítač s redukciou na PCMCIA funguje rovnako dobre. Viacerí výrobcovia (napr. Cisco a Agere) ponúkajú PCMCIA redukcie do PCI, alebo ISA špeciálne pre vloženie bezdrôtových kariet do stolných počítačov.



Pokiaľ je chipset na PCMCIA redukcii podporovaný pod Linuxom a samotná bezdrôtová karta má ovládače pre Linux, mala by Vaša bezdrôtová karta fungovať dobre. Nie je úplne nevyhnutné používať Orinoco bezdrôtovú kartu s Agere redukciou, napríklad.

Ak máte nejaké pochybnosti, či je Váš hardvér podporovaný pod Linuxom, pozrite si aktuálny Hardware HOWTO na <http://www.linuxdoc.org/HOWTO/Hardware-HOWTO/>.

Tiež by bolo dobré spomenúť, že existuje skupina starších kariet používajúcich frekvenciu podľa 802.11. Vyskytujú sa v oboch prevedeniach, PCMCIA aj ISA/PCI, ale nanešťastie nie sú kompatibilné s 802.11b. Ak chcete byť schopný podporovať 802.11b klientov a dátovú priepustnosť vyššiu ako 2Mbps, tak vám tieto karty nepomôžu. Vždy hľadajte to „b“, predtým než kúpite (to je dôvod prečo chlapík na počítačovej výstave predáva „bezdrôtové adaptéry“ za 20 USD).

Okrem PCMCIA slotu pre bezdrôtový adaptér budete potrebovať rozhranie na pripojenie ku druhej sieti. V laptope je to obvykle riešené sieťovou kartou v druhom PCMCIA slot, prípadne vstavaným modemom pre pripojenie k dial-up účtu. Pri stolnom, alebo regálovom počítači môže byť použitý akýkoľvek druh sieťového zariadenia, aj keď v súčasnosti je Ethernetová karta asi najbežnejšia (druhá možnosť len pre dial-up).

Pri tom ako napreduje súčasný hardvér môžete zvažovať použiť starší laptop ako bránu. Spotrebuje menej energie ako desktop, má zabudované záložné batérie a obvykle má dva PCMCIA sloty k dispozícii. Laptop 486 DX4/100 môže ľahko obsluhovať niekoľko ľudí, ako masquerading gateway (brána s tzv. maškarádou), pokiaľ má dostatok RAM (16 až 32 by malo byť dosť) a nerobí nič iné, než že smeruje pakety a poskytuje DHCP. Budeme navrhovať našu bránu tak, aby pracovala „bez hlavy“, takže dokonca ani funkčný LCD panel nebude podmienkou (predpokladáme, že Váš laptop má externý video konektor pre počiatočnú konfiguráciu). Často môžete zohnať staršie použité laptopy vo výpredajoch, alebo bazároch za cenu pod 200 USD (len ich pred kúpou určite vyskúšajte, musia bootovať!).

Veľkosť hard disku je vecou osobných priorít a toho, čo všetko chcete, aby brána urobila predtým, než poskytne prístup. Zatiaľ čo viac než kompletne distribúcie Linuxu môžu zaberať viac ako 2GB, plne funkčnú bránu môžete stlačiť do 20MB, alebo menej. V [odseku 5.1.10](#) na konci tejto kapitoly si ukážeme niekoľko príkladov distribúcií pre brány, ktoré sa celé zmestia na jediný floppy disk (žiadny hard disk nie je potrebný).

Samozrejme, ak už máte na Vašej sieti nejaký stroj poskytujúci služby firewallu, je to relatívne jednoduchá vec doinštalovať naň bezdrôtový adaptér a nechať ho slúžiť ako bránu. Ak už máte firewall bežiaci pod Linuxom, môžete kľudne preskočiť odsek Linuxové distribúcie.

Pre účely príkladu budem predpokladať, že sme nainštalovali kartu Orinoco Silver do laptopu s malým hard diskom a Ethernetovým pripojením na Internet.

5.1.2 Linuxové distribúcie

Výber distribúcie (veľmi podobné výberu operačného systému) by mal byť priamočiary proces: určiť ciele a požiadavky projektu, stanoviť čo ktorý výber poskytuje a urobiť rozhodnutie. Nanešťastie, konečný výber toho „jediného konkrétneho“ je zdá sa čoraz viac ovplyvňovaný marketingovou mašinériou a vášnivými debatami na Usenet-e, namiesto konkrétnych detailov koncepcie.

Namiesto odporúčania konkrétnej distribúcie Linuxu (a nechceného prezradenia môjho sklonu ku Slack-u) je tu niekoľko prvkov, ktoré sú životne dôležité pre bezdrôtovú bránu a mala by ich poskytovať Vaša distribúcia.

Toto sú povinné prvky:

- Linuxové jadro 2.2, alebo 2.4
- nástroje pre firewall (*ipchains*, alebo *iptables*)
- PCMCIA-CS
- balík bezdrôtových nástrojov - Wireless Tools
- nejaký DHCP server
- Váš obľúbený textový editor

Tieto prvky sú voliteľné:

- GCC, na kompilovanie ovládačov a nástrojov
- PPP, pre prístup k ISP pomocou dial-up
- SSH, pre vzdialenú administráciu

Tu sú veci, ktoré nebudete potrebovať (a pravdepodobne by len prekážali):

- X Windows, vrátane Gnome, KDE, alebo hocijakého iného správcu okien
- sieťové služby, ktoré neplánujete, že bude samotná brána poskytovať (NFS, Samba, tlačové služby, atď.)

Inštalácia Linuxu je pri väčšine moderných distribúcií úplne jednoznačná. Obvykle sa proces začne jednoducho nabootovaním z CD. V ďalšom budem predpokladať, že systém máte nainštalovaný a funkčný na Vašej existujúcej sieti. Ak potrebujete pomôcť, aby ste sa dopracovali k Vašej prvej výzve *login:*, existujú tony doporučení, online, ako nainštalovať Linux. Mohli by ste začať s informáciami, ktoré sú spracované v Linux Documentation Project na <http://www.linuxdoc.org/>.

5.1.3 Konfigurácia jadra

Keď už máte systémový softvér nainštalovaný, budete potrebovať nakonfigurovať jadro, aby poskytovalo bezdrôtové ovládače a služby firewallu. Parametre, ktoré si vyžadujú nastaviť, závisia na tom, ktoré jadro používate. Jadro 2.2 je uvoľnené už nejakú dobu a ukázalo sa ako stabilné v nespočítateľnom množstve vývojových prostredí. Jadro 2.4 bolo uvoľnené ako pre-release v januári 2001 a v čase písania knihy je aktuálne 2.4.5. Hoci je omnoho bohatšie čo sa týka vlastností a funkcionality, je tiež oveľa väčšie a zložitejšie. Pre novú inštaláciu na stroj s adekvátnou veľkosťou RAM (minimálne 16MB pre jednoduchú bránu) je jadro 2.4 asi tá najlepšia voľba, keďže čoraz viac vývojárov aktívne vyvíja ovládače pre túto platformu. Ak máte menej miesta, alebo máte stroj, s už

bežiacim jadrom 2.2, ktorý chcete zmeniť na bránu, potom v mnohých prípadoch funguje 2.2 výborne.

Teraz sa pozrime na špecifické parametre jadra, ktoré potrebujeme nastaviť pre každé jadro. V oboch prípadoch najskôr *cd* do */usr/src/linux* a spustíte *make menuconfig*. V týchto príkladoch budeme predpokladať, že používate buď 2.2.19, alebo 2.4.5. Kludne môžete skompilovať niektorú, alebo všetky tieto voľby ako zavediteľné moduly, je to použiteľné.

5.1.3.1 Linux 2.2.19

Uistite sa, že máte okrem ovládačov špecifických pre Váš hardvér (SCSI, alebo IDE zariadenia, štandardné súborové systémy, atď.), zakompilované do jadra aj nasledujúce parametre:

v časti *Loadable module support* (podpora zavediteľných modulov):

- Enable loadable module support (aktivovať podporu zavediteľných modulov)

pod *Networking options* (sieťové voľby):

- Packet socket (púzdrenie paketov)
- Network firewalls (sieťové firewally)
- Socket Filtering (puzdrové filtrovanie)
- IP: firewalling (tvorba IP firewallu)
- IP: masquerading (tvorba IP maškarády)
- IP: ICMP masquerading (ak chcete používať nástroje ako sú *ping* a *traceroute*)

pod *Network device support* (podpora sieťových zariadení):

- Wireless LAN (non-hamradio) (bezdrôtové lokálne siete)

Všimnite si, že potrebujete aktivovať len kategóriu Wireless LAN, a nie nejaký konkrétny ovládač. To aktivuje bezdrôtovú nadstavbu jadra a poskytne monitorovacie rozhranie */proc/net/wireless*. Nemajte obavy o sieťové ovládače PCMCIA, tieto poskytne balík PCMCIA-CS. Viac informácií nájdete neskôr v odseku PCMCIA-CS v tejto kapitole.

5.1.3.2 Linux 2.4.5

Skontrolujte, že nasledujúce voľby sú zabudované vo Vašom jadre:

Pod *Loadable module support* (podpora zavediteľných modulov):

- Enable loadable module support (aktivovať podporu zavediteľných modulov)

Pod *General setup* (všeobecné nastavenia):

- Support for hot-pluggable devices (podpora zariadení hot-plug)

Toto sprístupní kategóriu *PCMCIA/CardBus support* (podpora PCMCIA/CardBus). V tejto sekcii aktivujte nasledujúce:

- PCMCIA/CardBus support (podpora PCMCIA/CardBus)
- CardBus support (podpora CardBus) (len ak máte sieťovú kartu CardBus, napr. viaceré 100baseT karty)

- Podporu pre Váš PCMCIA premostovací (bridge) chipset. Viaceré sú i82365, aj keď vo všeobecnosti neublíži, ak sa skompilujú oba.

Pod *Networking options* (sieťové voľby):

- Packet socket (púzdrenie paketov)
- Socket Filtering (puzdrové filtrovanie)
- TCP/IP networking (tvorba sietí TCP/IP)
- Network packet filtering (filtrovanie sieťových paketov)

To sprístupní kategóriu *IP: Netfilter Configuration* (konfigurácia sieťového filtra). V tejto časti aktivujte nasledujúce:

- Connection tracking (stopovanie spojenia)
- FTP protocol support (podpora FTP protokolu)
- IP tables support (podpora IP tabuliek)
- Packet filtering (filtrovanie paketov)
- Full NAT (úplný NAT)
- MASQUERADE target support (podpora maškarády cieľa)

Pod *Network device support* (podpora sieťových zariadení) sú dve zaujímavé podkategórie. V časti *Wireless LAN (non-hamradio)* (bezdrôtové lokálne siete):

- Wireless LAN (non-hamradio)
- Hermes support (Orinoco/WavelanIEEE/PrismII/Symbol 802.11b card)

Podpora Orinoco a iných Prism II kariet zvykľa byť poskytovaná pomocou PCMCIA-CS (ako *wvlan_cs*), ale teraz sa presunula do samotného jadra (ako *orinoco_cs*). Aktivujte *Hermes support*, ak plánujete používať niektorú z týchto kariet. Prečo tento konkrétny ovládač sídli tu a nie pod *PCMCIA network device support* je záhada.

Keď už hovoríme o *PCMCIA network device support* (podpora sieťových zariadení PCMCIA), určite aktivujte nasledujúce:

- PCMCIA network device support (podpora sieťových zariadení PCMCIA)
- PCMCIA Wireless LAN (PCMCIA bezdrôtové lokálne siete)
- hocikaké PCMCIA sieťové ovládače pre Váš hardvér

Okrem vyššie požadovaných komponentov tiež zahrňte ovládače, ktoré potrebujete pre Váš špecifický hardvér. Ak je to po prvý krát čo zostavujete nové jadro, pamätajte na to, aby ste zo začiatku všetko definovali jednoducho. Oslnivý sortiment volieb jadra môže miasť a pokúšať sa urobiť príliš veľa vecí naraz, môže viesť ku konfliktom, ktoré je problematické vyriešiť. Jednoducho zahrňte len minimum funkcionality, ktorú potrebujete na to, aby stroj bootoval a pracoval so sieťou a pridávajte vyšperkovanú funkcionality neskôr. Dokumentačný projekt Linuxu má niekoľko ohromných referencií a materiálov typu kuchárskych kníh v Kernel HOWTO (ako na jadro) na <http://www.linuxdoc.org/HOWTO/Kernel-HOWTO.html>. RTFM⁹ a doporučte ostatným urobiť to isté !

9 Read The Fine Manual (prečítajte si skvelý manuál). Vďaka snahe skupín dobrovoľníkov, ako je LDP (Linux Documentation Project) a tisíckam prispievateľov, stal sa Linux snáď najlepšie zdokumentovaným operačným systémom na Zemi. Akde skvelý manuál nie je dostupný, existuje zdroják. Čítajte.

5.1.4 PCMCIA-CS

PCMCIA a kartové služby (Card Services) poskytujú podporu operačného systému pre všetky druhy zariadení veľkosti kreditnej karty, vrátane Ethernetu a bezdrôtových kariet. Balík PCMCIA-CS v súčasnosti pozostáva z dvoch častí, samotných ovládačov a utilít, ktoré riadia zavádzanie a odstraňovanie daných ovládačov. Utility detekujú keď sú karty zasunuté, alebo vysunuté a dokážu Vám podať informáciu o tom, čo bolo detekované.

5.1.4.1 Softvér

Ak Vaša distribúcia obsahuje čerstvé vydanie PCMCIA-CS, kľudne preskočte tento odsek. Zistiť ktorú verziu máte nainštalovanú môžete spustením `/sbin/cardmgr -V`. Úspešne som používal 3.1.22 a 3.1.26. Posledné (a odporúčané) vydanie v čase písania tejto knihy je 3.1.26.

Ak potrebujete upgradovať Váš PCMCIA-CS, nasledujte inštalačné inštrukcie v balíku (vychádzajú spolu s aktuálnym PCMCIA-HOWTO). Keď ho zostavujete zo zdrojákov, balík predpokladá, že máte strom Vášho jadro po ruke, preto najskôr zostavte Vaše jadro a následne PCMCIA-CS. Posledné vydanie môžete stiahnuť z <http://pcmcia-cs.sourceforge.net/>.

5.1.4.2 Konfigurácia

Nastavovanie rádiových parametrov je jednoznačné. Všetky bezdrôtové parametre sú nastavené v `/etc/pcmcia/wireless.opts`.

Tu je príklad `wireless.opts`:

```
#
# wireless.opts
#

case "$ADDRESS" in
  *,*,*,*)
    INFO="Default configuration"
    ESSID="NoCat"
    MODE="Ad-Hoc"
    RATE="auto"
    ;;
esac
```

Možno si myslíte, „pre pána Jána, je to plné hviezdičiek, ...“. Ale ak ste už niekedy pracovali s `network.opts`, syntax je presne tá istá. Ak ešte nie, tak tie hviezdičky umožňujú úžasnú flexibilitu.

Skriptu je predávaný refazec cez `$ADDRESS`, ktorý obsahuje detaily o karte, ktorá bola zasunutá, takže môžete mať rôzne odseky pre rôzne karty. Syntax súvisiaca s adresou je:

```
scheme,
socket,
instance,
MAC address)
```

Scheme umožňuje nastaviť toľko ľubovoľných profilov, koľko chceme. Najbežnejšie použitie pre *scheme* je na klientskom laptope, kde môžete mať odlišné sieťové nastavenia pre firemnú bezdrôtovú sieť, než pre Vašu domácu sieť. Zobrazíť aktuálnu schému môžete zadaním príkazu *cardctl scheme* ako root a môžete ju zmeniť použitím príkazu ako *cardctl scheme home*, alebo *cardctl scheme office*. Obidva *wireless.opts* aj *network.opts* sú si schémy uvedomujúce a umožňujú Vám meniť sieťové a bezdrôtové nastavenia rýchlo, jedným príkazom.

Druhý parameter, *socket*, je číslo zásuvky do ktorej bola PCMCIA karta zasunutá. Obvykle začína s 0 a pokračuje až po počet PCMCIA slotov ktoré máte. Kvôli zisteniu ktorý je ktorý, zasunúť kartu do niektorého slotu a zadajte príkaz *cardctl status*.

Tretí parameter, *instance*, je použitý pre exotické sieťové karty, ktoré majú viac ako jedno rozhranie. Neprišiel som do styku so žiadnou z týchto kariet, ale ak máte sieťovú kartu, ktorá má v sebe viac ako jedno sieťové zariadenie, použijete toto na nastavenie rozdielnych parametrov pre každé zariadenie, začínajúc s 0.

Posledný parameter, *MAC address*, považujem za veľmi užitočný, pretože môžete spojiť nastavenia so špecifickou MAC adresou. Dokonca môžete začleniť zástupné znaky na porovnanie s čiastočnou MAC adresou, takto:

```
*,*,*,00:02:2D:*)
```

Tomuto vyhovie každá súčasná Lucent karta, vložená v ktoromkoľvek slotu a pri hocijakej schéme. Pamätajte, že *wireless.opts* je volané len pre nastavenie rádiových parametrov. Sieťové nastavenia (ako je IP adresa, predvolená brána, a či použiť DHCP alebo nie) sú nastavené v *network.opts*.

Pre náš príklad bezdrôtovej brány budeme potrebovať nastaviť Ethernetovú kartu a Orinoco Silver kartu. Vložte vyššie uvedený kód do Vášho *wireless.opts*. Vytvorte nasledovné odseky vo Vašom *network.opts*:

```
*,0,*,*)
    INFO="Wired network"
    DHCP="y"
;;
*,1,*,*)
    INFO="Wireless"
    IPADDR="10.0.0.1"
    NETMASK="255.255.255.0"
    NETWORK="10.0.0.0"
    BROADCAST="10.0.0.255"
;;
```

Určite to zadajte nad odsek začínajúci **,*,*,*)*, pretože inak to bude mať prednosť pred Vašimi špecifickými nastaveniami. Tieto nastavenia predpokladajú, že káblová sieť získa IP adresu cez DHCP. Môžete nastaviť *DHCP="n"* (alebo len vymazať riadok) a zadať IP adresu (ako je v druhom príklade) ak Váš ISP používa statické IP adresy. Príklady predpokladajú, že Ethernetová karta je v slotu 0 a rádiová v slotu 1. Tiež sa môžete odvolávať na MAC adresu Vašich kariet, ak chcete flexibilitu pre vloženie hociktovej karty do hociktorého slotu, hoci obvykle, keď už raz máte bránu vytvorenú a fungujúcu, budete to chcieť dokonca zabudnúť. Pozri PCMCIA HOWTO pre viac detailov o rôznych trikoch, ktoré môžete robiť s *\$ADDRESS*.

5.1.5 Wireless Tools (bezdrôtové nástroje)

Vynikajúci balík Wireless Tools spravuje Jean Tourrilhes. Kópiu môžete získať online z http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html. Autor popisuje balík nasledovne:

Wireless Extension (bezdrôtová nadstavba) je všeobecné API umožňujúce ovládaču ukázať sa pre konfiguráciu užívateľského priestoru a štatistiky špecifické pre bežné bezdrôtové lokálne siete.

Tieto nástroje poskytujú metódy riadenia parametrov bezdrôtových kariet, bez ohľadu na to, aký typ karty je inštalovaný (predpokladajúc, že ovládač bezdrôtovej karty používa bezdrôtové rozšírenie jadra). Umožňujú Vám nastaviť ESSID, WEP kľúče, operačný mód (BSS, alebo IBSS), kanál, módy šetrenia energie a množstvo ďalších volieb. Jednoducho rozbaľte archív a spustíte *make*, *make install* by mal skopírovať binárne súbory do */usr/local/sbin* (viac informácií nájdete v inštalačných poznámkach v balíku). Nástroje, ktoré sú momentálne vo verzii 21, obsahujú *iwconfig*, *iwspy*, *iwlist* a *iwpriv*. Sú absolútne nevyhnutné pre každú Linuxovú bránu, alebo klienta.

Rovnako, ako jeho náprotivok *ifconfig*, nástroj *iwconfig* pracuje na špecifickom rozhraní a umožní Vám prezerať a meniť jeho parametre. Spustíte ho môžete kedykoľvek z príkazového riadku, ako root, aby ste videli čo sa deje. Na dôvažok, PCMCIA-CS volá *iwconfig*, keď je zasunutá karta, aby sa nastavili východiskové parametre.

Tu je typický výstup *iwconfig*:

```
root@entropy:~# iwconfig eth0
```

```
eth0      IEEE 802.11-DS  ESSID:"NoCat"  Nickname:"Entropy"
          Mode:Ad-Hoc  Frequency:2.412GHz  Cell: 00:02:2D:FF:00:22
          Bit Rate:11Mb/s  Tx-Power=15 dBm  Sensitivity:1/3
          RTS thr:off  Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality:56/92  Signal level:-40 dBm  Noise level:-96 dBm
          Rx invalid nwid:0  invalid crypt:0  invalid misc:0
```

Ako vidíte *eth0* je bezdrôtové zariadenie. ESSID je nastavený na „NoCat“ a WEP šifrovanie je vypnuté. Z bezpečnostných dôvodov je šifrovací parameter zobrazený len ak *iwconfig* spustí root. Ak sú nejaké ďalšie bezdrôtové karty v dosahu s nastavenými rovnakými parametrami, môžu „vidieť“ tento uzol a zahájiť komunikáciu presne tak isto, ako keby boli na tom istom fyzickom kuse drôtu. Spustíte *man iwconfig* a získate úplný zoznam parametrov. Binárny súbor *iwconfig* by mal byť v spoločnej ceste (path) k binárkam (ako */usr/sbin*, alebo */usr/local/sbin*), aby ho bolo PCMCIA-CS schopné používať.

Ďalšie nástroje majú veľmi dobré schopnosti, ako je monitorovanie relatívnej sily signálu ďalšieho IBSS uzla, zobrazovanie dostupných frekvencií a dekodovanie vzorkovania (bit rates) a dokonca nastavovanie interných parametrov ovládača, všetko z príkazového riadku. V dokumentácii nájdete všetky detaily a v [kapitole 7](#) je niekoľko príkladov.

Pre veľa činností týkajúcich sa bezdrôtovej brány, poskytuje *iwconfig* všetku funkcionálnu, potrebnú pre programovanie bezdrôtovej karty. Keď už ste na stránke

Jeana Tourrilhesa zoberte si tiež *hermes.conf* a skopírujte ho do */etc/pcmcia*. Povie PCMCIA aby používal nový ovládač *orinoco_cs* (radšej než starší *wvlan_cs*) pre všetky kompatibilné rádia. Viac detailov nájdete na jeho dokumentačnej stránke.

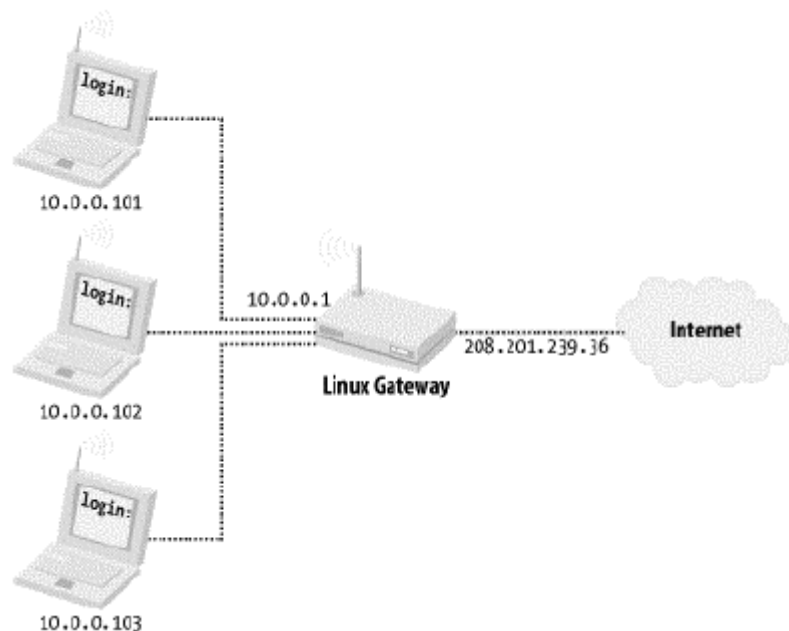
5.1.6 Maškaráda

Z IP Masquerade HOWTO (dostupné na <http://www.linuxdoc.org/HOWTO/IP-Masquerade-HOWTO.html>):

IP maškaráda je forma prekladu sieťových adries (Network Address Translation), alebo NAT, ktorá dáva interne pripojeným počítačom, ktoré nemajú jednu, alebo viac registrovaných Internetových IP adries, schopnosť komunikovať cez Internet, pomocou jednej Internetovej IP adresy Vašej Linuxovej skrinky.

S IP maškarádou je takmer triviálne dať celej súkromnej sieti prístup na Internet, hoci aj len s použitím jedinej oficiálnej registrovanej IP adresy.

Nakonfigurovaním káblového Ethernetu brány tak, aby používal Vašu, od ISP pridelenú, adresu a aktivovaním maškarády medzi káblom a bezdrôtovými zariadeniami, všetci Vaši bezdrôtoví klienti môžu zdieľať Internetové pripojenie, tak ako je to znázornené na [obrázku 5-1](#). Interné počítače si myslia, že sú pripojené priamo na Internet a pritom nie je potrebné vykonať žiadne špeciálne nastavenia nejakej aplikácie (ako by ste potrebovali pri tradičnom proxy serveri).



Obrázok 5-1. Použitie maškarády, celá súkromná sieť môže byť „skrytá“ za jedinou reálnou IP adresou.

Tak ako každá forma NAT-u, aj maškaráda má svoje tienisté stránky. Napr. pripojenie je jednosmerné na začiatku. Interné počítače sa môžu pripojiť ku Internetovým zdrojom, ale užívatelia z Internetu sa nemôžu pripojiť priamo ku interným uzlom.

Pre nakonfigurovanie maškarády pre jadro 2.2.19, uložte nasledujúci skript do */etc/rc.d/rc.firewall* a pridajte jeho vyvolanie vo Vašom štartovacom skripte */etc/rc.d/rc.local*:

```
#!/bin/sh

echo "Enabling IP masquerading..."

# Set the default forwarding policy to DENY
/sbin/ipchains -P forward DENY

# Enable masquerading from the local network
/sbin/ipchains -A forward -s 10.0.0.0/24 -j MASQ

# Turn on forwarding in the kernel (required for MASQ)
echo "1" > /proc/sys/net/ipv4/ip_forward
```

V Linuxe 2.4.5 inštalujte tieto príkazy na rovnaké miesto, ale použite *iptables* na nastavenie pravidiel maškarády:

```
#!/bin/sh

echo "Enabling IP Masquerading..."
/sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

# Turn on forwarding in the kernel (required for MASQ)
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Určite zameňte *eth0* za meno rozhrania Vašej bezdrôtovej karty. Kópiu týchto vzorových skriptov môžete získať na <http://www.oreilly.com/catalog/wirelesscommnet/>.

Tieto pravidlá umožnia hocikomu v dosahu Vášho rádia maškarádu za Vašou živou IP adresou a prístup na Internet, ako keby bol k nemu priamo pripojený.

5.1.7 DHCP služby

Ako bolo popísané v [kapitole 3](#), DHCP umožňuje sieťovým klientom automaticky zistiť zodpovedajúce sieťové parametre, bez zásahu človeka. Ak chceme, aby naši bezdrôtoví klienti používali DHCP, je potrebné to poskytovať na bezdrôtovom rozhraní.



Možno si myslíte, „Prečo jednoducho nepremosťť dané dve siete spolu a nepoužívať existujúce DHCP služby mojej siete?“. Nanešťastie, mnoho 802.11b výrobcov (vrátane Lucent) dospelo k presvedčeniu, že ak Layer 2 premostovanie (druhá vrstva - linková) bude možné v ich klientských kartách, potom bude len veľmi malá potreba ich high-end (a drahých) AP. Výsledkom je, že schopnosť premostovania bola deaktivovaná firmvérom klientskej karty. Niektorí výrobcovia (najmä Cisco) stále umožňujú premostovanie na linkovej vrstve.

Štandardný DHCP server bol napísaný organizáciou Internet Software Consortium. Ak nie je súčasťou Vašej distribúcie, zoberte si kópiu z <http://www.isc.org/products/DHCP/>. Konfigurácia je jednoznačná. Jednoducho vytvorte */etc/dhcpd.conf* s nasledujúcimi informáciami:

```

subnet 10.0.0.0 netmask 255.255.255.0 {
    range 10.0.0.100 10.0.0.200;
    options routers 10.0.0.1;
    options domain-name-servers 1.2.3.4;
}

```

Nahradíte 1.2.3.4 Vaším lokálnym DNS serverom.

Keď už je to na mieste, pridajte odsek do Vášho `/etc/rc.d/rc.local` skriptu, aby zavolať `dhcpd` na bezdrôtovom rozhraní. Keď predpokladáme, že Vaša bezdrôtová karta je na `eth0`, toto by to malo urobiť:

```

echo "Starting dhcpd..."
/usr/sbin/dhcpd eth0

```

Ak sa `dhcpd` sťažuje na chýbajúci súbor `dhcp.leases`, skúste `touch /var/state/dhcp/dhcpd.leases` ako root a naštartujte ho znova. Pozrite sa do dokumentácie na viac techník pomoci v núdzi (troubleshooting) a príkladov, vrátane nastavenia statických licencií (leases), WINS serverov, skupín a všetkých druhov vecí o ktorých ste možno nikdy nepočuli, že by mohol byť DHCP server schopný.



Uistite sa, že spúšťate `dhcpd` na Vašom bezdrôtovom rozhraní a nie na kábli! Pretože DHCP je vysielací protokol, sieť môže mať maximálne jeden DHCP server. Viac ako jeden môže zapríčiniť všetky druhy sieťového chovania sa, ako dva kohúty, vždy keď klient požaduje DHCP licenciu.

Nie je dostupných veľa slobodných alternatív ku štandardnému ISC `dhcpd`. Jeden zaujímavý balík vydal Moreton Bay, výrobca vnorených systémov. Vydali ich `dhcpd` balík pod GPL. Hoci on nemá takmer zvončeky, písanie a vibra-slaps (<http://www.helixmusic.com.au/vibraslap.htm>) ISC implementácie, naozaj poskytuje jednoduché DHCP služby veľmi, veľmi rýchlo. Kópiu môžete získať na <http://www.moretonbay.com/dhcpd/>. Konfigurácia je mierne obmedzená (je to zreteľne navrhnuté pre beh vo vnorenom prostredí, keďže používa malé binárne konfiguračné súbory).

5.1.8 Bezpečnosť

Príklady uvedené vyššie vytvárajú jednoduchú, otvorenú konfiguráciu brány. Ak sa nestaráte o to, kto sa spája s Vašou bránou (a používa Vašu sieť), mala by predchádzajúca konfigurácia pre Vás fungovať vyhovujúco. Príkladom takéhoto verejného prístupu by mohla byť konferencia, alebo stretnutie skupiny užívateľov, kde sa bude veľa klientov pripájať ku sieti a jednoduchosť pripojenia je prvoradý záujem.

Za iných okolností možno nechcete dovoliť žiadnemu cudzincovi používať Vašu sieť. Predstavme si, že chcete bezdrôtovú bránu pre Vašu domácu sieť a nastavili ste bránu tak, aby používala externé IP adresy Vašej DSL linky. Hocikto, kto bol v dosahu Vášho rádia, sa mohol potenciálne pripojiť, čerpať šírku pásma a dokonca posilať spam, alebo napadnúť ostatné stroje v sieti. Všetok tento traffic by pochádzal z Vašej IP adresy, za ktorú ste zmluvne (nemyslím sociálne) zodpovedný.

Ak chcete jednoducho umožniť prístup sebe a Vaším priateľom, aktivovanie WEP šifrovania môže poslúžiť ako ľahký a efektívny strašiak na možných lupičov. Pri používaní WEP, všetci klienti, ktorí sa chcú navzájom rozprávať, musia používať ten istý

kľúč. V mnohých klientoch to môže byť špecifikované buď ako hexadecimálne číslo, alebo ako ASCII reťazec. Dĺžka kľúča je závislá od úrovne šifrovania ktorú chcete používať. Špecifikácia 802.11b pripúšťa 40 bitové kľúče, ktorých používanie umožní každému druhu hardvéru, ktorý spĺňa podmienky tejto špecifikácie, komunikovať medzi sebou. Niektorí výrobcovia vydali ich vlastnú 128 bitovú implementáciu šifrovania, ale keďže to nie je časť súčasného štandardu, takéto karty budú fungovať len so zariadeniami od toho istého výrobcu.

Ja vysoko doporučujem používať 40 bitové šifrovanie pre jednoduchú kontrolu prístupu, keďže to spôsobí menej problémov ohľadom kompatibility v budúcnosti. (Pozrite si rôzne čerstvé príspevky ohľadom odôvodnenosti implementácie WEP, jednoduché pridanie viacerých bitov do kľúča nevyhnutne neurobí veľa pre väčšiu bezpečnosť.¹⁰)

Pre použitie 40 bitového kľúča v Linuxe, zadajte buď 5 znakový reťazec, alebo 10 číslíkové hexadecimálne číslo, ako parameter *enc* do *iwconfig*. Veľa ľudí rado používa reťazce, pretože sú ľahšie na zapamätanie. Ak chcete použiť ASCII reťazec, musíte pred neho dať *s:*, aby ste oznámili *iwconfig*-u, že nasleduje reťazec. Ak chcete kľúč nastaviť na ASCII reťazec *pLan9*, mohli by ste použiť jeden z týchto dvoch príkazov:

```
root@gateway# iwconfig eth0 enc s:pLan9
root@gateway# iwconfig eth0 enc 704C-616E-39
```

Všimnite si, že keď používate ASCII kľúč, tak kľúč rozlišuje veľké a malé písmená.

Aby ste aktivovali WEP na vašej bráne už pri bootovaní, zeditujte Váš */etc/pcmcia/wireless.opts* tak, že pridáte riadok *KEY=* do bezdrôtovej časti, podobne:

```
KEY="s:pLan9"
```

Pamätajte, že keď robíte zmeny v súboroch v */etc/pcmcia/*, je nevyhnutné zastaviť a spustiť pcmcia služby (alebo reboot), predtým než sa zmeny stanú platnými. Všetky detaily, ako nastaviť *wireless.opts*, nájdete v [odseku 5.1.4](#).

Keď už raz máte Vašu bránu nastavenú, dajte Váš vlastný kľúč všetkým bezdrôtovým klientom, ktorým chcete dať prístup. Pokiaľ súhlasia ESSID a WEP kľúče, môžete mať súkromnú sieť, ktorá poskytuje Internetový prístup. Ostatné rádia vo Vašom dosahu nemôžu používať Vašu bránu bez týchto informácií.

Ak je Vaším cieľom ponúkať sieťový prístup Vašej lokalite bez toho, aby ste sa vystavili riziku, alebo poskytnúť všetku Vašu šírku pásma, pozrite sa na „catch and release“ portál v [kapitole 7](#).

5.1.9 Spájanie všetkého dohromady

Rekapitulácia všetkého čo je potrebné pre výstavbu brány:

1. Inštalovať hardvér.
2. Konfigurovať jadro.
3. Upgrade PCMCIA-CS, ak je to potrebné.

¹⁰ Najmenej 4 dokumenty o zraniteľnosti WEP sú dostupné online na

<http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>,

<http://www.cs.umd.edu/~waa/wireless.pdf>, <http://www.cs.rice.edu/~astubble/wep>

a http://www.cryptocom/papers/others/rc4_ksaproc.ps.

4. Inštalovať Wireless Tools (bezdrôtové nástroje).
5. Skontrolovať `/etc/pcmcia/wireless.opts` a `network.opts`, nastaviť ESSID, sieťové parametre, a WEP kľúče (ak je to potrebné).
6. Nastavenie pravidiel firewallu pre maškarádu.
7. Nastaviť `dhcpcd`, aby sa spúšťal pri bootovaní.

Keď už je všetko na svojom mieste, rebootujte bránu, aby ste sa uistili, že všetko sa inicializuje správne, bez ľudského zásahu. Gratulujeme, teraz máte bezdrôtovú bránu!

5.1.10 Predpripravené Linuxové Distribúcie

Teraz, keď sme prešli cez všetko úsilie výstavby našej vlastnej brány, môže byť pre Vás zaujímavé vedieť, že ostatní to nie len už urobili, ale tiež podávajú ďalej ovocie svojej snahy. Obrovská výhoda natlačenia minimálnej Linuxovej inštalácie s bezdrôtovými ovládačmi na disketu je prenosnosť, s floppy diskom môžete zmeniť hociktorý šikovný laptop na bezdrôtovú bránu. Samozrejme, postrádajú flexibilitu plnej inštalácie Linuxu, ale dokážu byť veľmi šikovné v neočakávaných situáciách.

Pozrite si tieto brána-na-diskete distribúcie:

The Linux Router Project (LRP)

Jedna z prvých Linuxových distribúcií na floppy disku, teraz s ovládačmi bezdrôtovej siete: www.linuxrouter.org/

The Wireless Router Project (WRP)

Pôvodne založený na LRP, neskôr prepísaný a optimalizovaný na stavbu bezdrôtových brán: <http://www.nocat.net/>

Kapitola 6. Nasýtenie rozľahlých sietí

Máte prístupový bod - AP. Váš laptop svižne bzučí. Zatiaľ čo práca doma, alebo v kancelárii je omnoho pružnejšia než kedykoľvek predtým, pristihnete sa ako rozmýšľate nad tým, koľko by to trvalo dostať signál naproti cez ulicu, do Vašej obľúbenej kaviarne.

Alebo možno bývate v oblasti, kde ste ustavične na zozname „vrátime sa k Vám“ širokopásmových služieb, ako DSL a káblový modem a ste pripravený to zrealizovať teraz. So správnym zariadením, dostatkom účastníkov a spolupráce sa naozaj môžete stať širokopásmový Internetový prístup vo Vašich končinách realitou.

Bez ohľadu na Vašu motiváciu, hľadáte spôsob ako zväčšiť dosah 802.11b nad spomínanú hranicu 300 metrov. To je nie len možné a úplne legálne, ale je to aj veľmi zábavné. Predovšetkým si musíte ujasniť, aká je Vaša cieľová oblasť pre pokrytie signálom a aké zdroje potrebujete na to, aby ste to zrealizovali.

Zatiaľ čo rozšírenie Vašej súkromnej siete o ulicu, alebo dve (alebo dokonca o niekoľko kilometrov, s príslušnými anténami) môže byť zaujímavé pre Vás, nerobí nič pre ostatných vôkol Vás, okrem vytvárania väčšieho šumu v pásme. Veľa ľudí zistilo, že je neskutočne drahé prenajať si mestský priestor a vytvoriť sieťový prístup pre seba, kdekoľvek sa v meste ocitnú. To viedlo k úchvatnému fenoménu spolupracujúcich bezdrôtových sietí.

Najlepšia rada akú Vám viem dať na Vašu cestu za najlepšou sieťou (či už verejnou, alebo súkromnou) je bojovať s naliehavosťou všetko to slepo urobiť sám. Zatiahnite do toho ľudí z najbližšieho okolia. Zvolajte schôdzu zainteresovaných. Nájdite ďalších ľudí vo Vašej oblasti, ktorí majú podobné ciele a spojte Vaše sily. Ak tam žiadny nie sú, navštívte niektorú väčšiu diskusnú skupinu ohľadom komunitných sietí (pozri [prílohu A](#)) a popýtajte sa. Šance sú, iný dosiahlí (alebo to zamýšľajú urobiť) to čo chcete Vy a možno budú radi, ak Vám budú môcť poskytnúť svoje skúsenosti.

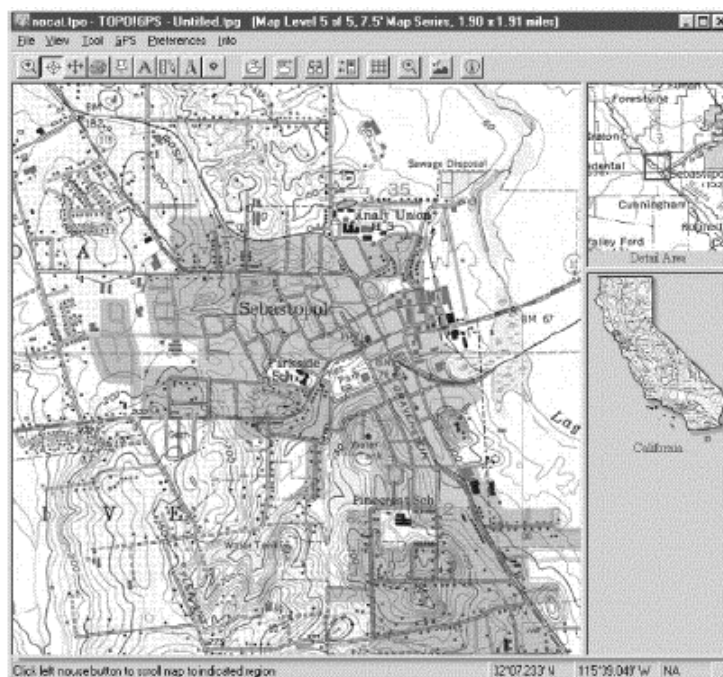
Ako narastá počet ľudí zaujímavujúcich sa o prístup k bezdrôtovým sieťam, siete s verejným prístupom začali mať úžitok z prístupu k výhodnejšie umiestneným bodom, obrazne aj fyzicky. Hoci Vy snáď nemáte priamu viditeľnosť na miesto s ktorým chcete komunikovať, Váš sused ju môže mať. A ak dostane zdarma prístup ku sieti, možno Vás nechá namontovať nejaké zariadenia a použiť svoj dom ako repeater. Bezdrôtová šírka pásma stojí len elektrinu a zariadenia, žiadne poplatky telefónnym, alebo káblovým spoločnostiam. Toto silne paralelné, spolupracujúce usporiadanie je to, čo robí vysokorýchlostné rozľahlé siete možnými. Avšak ja Vám môžem dať len technické detaily, sociálne aspekty sú ponechané ako úloha pre čitateľov.

6.1 Topo Maps 102: Vysporiadanie sa s geografickou rozmanitosťou

Ak chcete natiahnuť Váš signál ďalej než len naproti cez ulicu, musíte zvážiť čo presne leží medzi danými bodmi Vašej siete. V [kapitole 2](#) sme si ukázali použitie USGS topografických máp a DOQ na určenie, aký je profil terénu medzi dvoma ľubovoľnými bodmi. Nadôvažok ku papierovým a online topografickým mapám pribudne v priebehu niekoľkých rokov verzia na CD-ROM. Hoci je typicky vytváraná pre turistov, má čo ponúknuť inžinierom usilujúcim sa o rozľahlú sieť.

6.1.1 Softvér

Testoval som dva populárne komerčné topo balíky, Topo! od National Geographic a DeLorme's TopoUSA 2.0. [Obrázok 6-1](#) znázorňuje Topo! stvárajúci Sebastopol v Kalifornii. Hoci sú oba distribuované spolu s funkciami, len pár ich je priamo použiteľných na to, aby Vám pomohli analyzovať krajinu medzi dvoma bodmi.



Obrázok 6-1. Topo! stvárajúci Sebastopol.

Tu je pár bodov, na ktoré je dobré pamätať, pri hodnotení topo softvéru pre analýzu spojení:

- Softvér by mal poskytovať prierezové pohľady z daného smeru, alebo nakreslenej trasy. To je asi najčastejšie používaná funkcia, keď sa pokúšate zistiť, či má krajina vhodný tvar (pozri príklady v nasledujúcom odseku).
- Takmer každý lepší balík topo softvéru obsahuje schopnosť pridávať značky s textom a bodmi ku mape. Schopnosť importovať lat/lon dáta a prekladať ich na dátové body je šikovná, ak poznáte polohu len podľa jej zemepisnej šírky a dĺžky (latitude a longitude).
- Ak máte v úmysle používať GPS so svojím softvérom (viď nasledujúci odsek), presvedčte sa, že Váš topo softvér podporuje Váš GPS hardvér. Oba balíky, ktoré som testoval, podporujú mnoho populárneho GPS hardvéru a NMEA dátový štandard (ktorým komunikujú prakticky všetky moderné GPS prijímače).
- Oba balíky, ktoré momentálne používam, sú len pre Windows. Existuje veľa Linuxových mapových balíkov, ktoré stvárnajú USGS DOQ a DEM, ale tak ako mnoho Linuxového softvéru, môže to vyžadovať pár figľov, aby ste ich rozchodili. Prezrite si linky na mapové zdroje na stránkach významných bezdrôtových komunit (viď [príloha A](#)), je to priestor pre prudký vývoj v open source komunitě.

Akýkoľvek softvér si vyberiete, mal by Vám uľahčiť, aby ste s ľahkosťou rozoznali očividne neuskutočniteľné priame spojenia. Ak dospejete ku „snáď“ (čo je najčastejší prípad), neostáva Vám iné, ako ísť von a vyskúšať to. Samozrejme, pre mnohých z nás je to zábavná časť.

6.1.2 Používanie GPS na záznam prípadných Lat/Lon/Alt

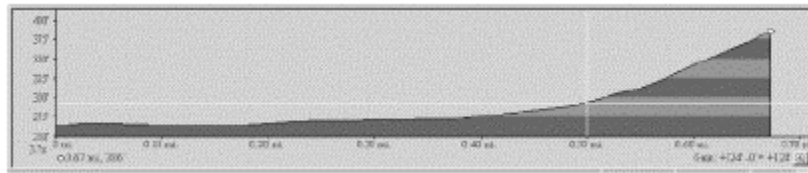
(latitude/longitude/altitude - zemepisná šírka/dĺžka/nadmorská výška)

Kdekoľvek som navštívil potenciálne miesto pre uzol, priniesol som si môj GPS so sebou. Zaznamenáva nie len (viac, alebo menej) presnú zemepisnú šírku a dĺžku, ale aj nadmorskú výšku miesta. To sú údaje, ktoré môžete vyčítať s topo mapy, ale hodí sa mať presné meranie (obzvlášť, ak ste zaznamenali viac bodov na Vašej zamýšľanej sieťovej trase). [Obrázok 6-2](#) znázorňuje použitie GPS na označenie potenciálnej polohy.



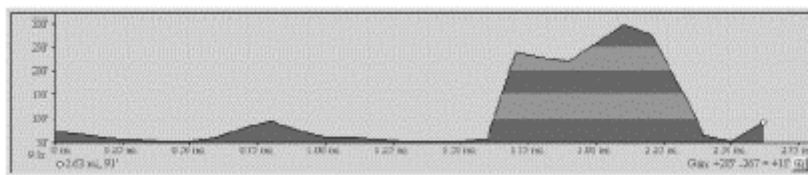
[Obrázok 6-2](#). Môžete použiť GPS na označenie potenciálnych miest a analyzovať ich neskôr pomocou softvéru.

Po zozbieraní bodov ich môžete načítať do Vášho topo softvéru a vykresliť. Nakreslite trasu medzi nimi, aby ste zistili, aký profil má terén medzi danými dvoma bodmi. [Obrázok 6-3](#) zobrazuje Topo! stvárnajúce polohu. Na základe tohto zobrazenia by malo byť spojenie malinou.



Obrázok 6-3. Dobrý topo softvér, by mal byť schopný, poskytnúť prierez terénom, medzi hocijakými dvoma bodmi.

Pamätajte, že aj keď daný topo softvér prehliada geologické údaje, nebude mať informácie o stromoch, alebo budovách. Môžete získať všeobecnú predstavu o tom, ako je prepchatá oblasť, ale nebudete to presne vedieť, pokiaľ neskúsíte spojenie. Použitie pôdorysu v kombinácii s prierezom môže nie len odstrániť očividné negatíva, ale tiež nájsť potenciálnu možnosť. **Obrázok 6-4** zobrazuje polohu, ktorá by nemala byť použiteľná. Snáď môžete ísť okolo? Mimochodom, kto býva na tom kopci?

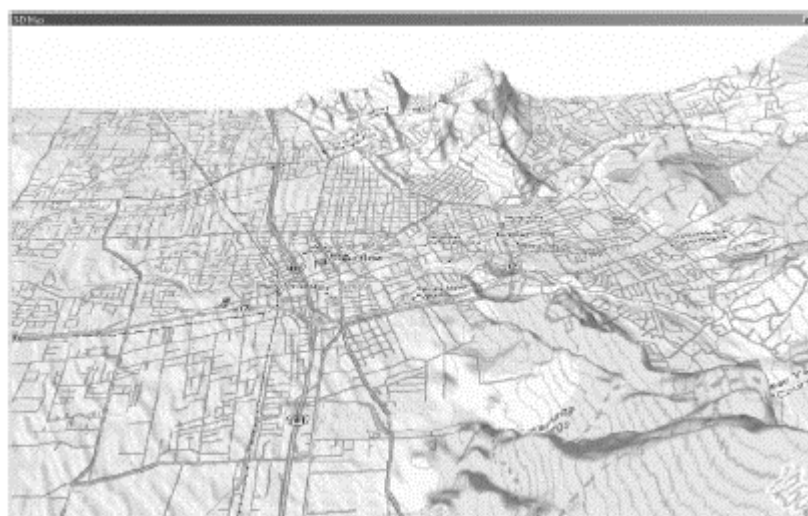


Obrázok 6-4. Tento prierez zobrazuje nočnú moru dlhej vzdialenosti: žiadna šanca.

Použitie pôdorysu na umiestnenie kľúčových bodov pre repeatre môže byť zábava. Zistíte kde je dobrá poloha a pokúste sa kontaktovať ľudí na týchto miestach. Vo väčšine prípadov ľudia budú spolupracovať s miestnou komunitou, aby poskytli voľný prístup (najmä ak nemusia robiť nič, okrem poskytnutia elektriny a ak navyše môžu získať vysokorýchlostný prístup zdarma).

6.1.3 Vykresľovanie bodov do 3D mapy

DeLorme má zaujímavú schopnosť vytvoriť 3D stvárnenie topo regiónu, kompletne s dátovými značkami a návestiami. **Obrázok 6-5** zobrazuje toto stvárnenie. Hoci je tento prvok naozaj cool (a veľmi príťažlivý pri prezentáciách), má obmedzenú praktickú hodnotu, okrem pomoci pri zobrazení okolitého terénu. Samozrejme, ak máte celý húd dátových bodov, dokáže vytvoriť pôsobivú vizuálnu prezentáciu.



Obrázok 6-5. TopoUSA od DeLorme Vám poskytuje 3D stvárnenie akéhokoľvek topo regiónu, kompletne s dátovými bodmi.

Keď už sú body vykreslené na mape, dokážete veľmi rýchlo rozhodnúť, ktoré miesta sú horšie pre výstavbu. Ak nemáte priamu viditeľnosť na miesto, na ktoré by ste chceli, pozrite si okolitú geografiu a zvážte, či nenájdete inú cestu. Ak nemôžete ísť cez, budete musieť ísť ponad, alebo popod. Softvérové topo mapy dokážu hľadanie veľmi uľahčiť.

6.2 Charakteristiky antén a ich umiestnenie

Hoci nie som rádio frekvenčný (RF) inžinier, získal som mnoho praktických skúseností pri výstavbe 802.11b sietí. Tu nie je dostatok priestoru na úplné preskúmanie všetkých nuáns rádiových komunikácií. Aby ste získali spoľahlivejšie materiály, určite si pozrite úžasné zdroje v [prílohe A](#), menovite ohromnú publikáciu vypracovanú organizáciou American Radio Relay League (AARRL), čo je asociácia rádio amatérov. Rádio samo o sebe je samostatná oblasť na štúdium.

Výber antény má obrovský dopad na dosah a použiteľnosť Vašej bezdrôtovej siete. Paradoxne, tvar takmer všetkých externých 802.11b kariet stavia antény do najhoršej možnej orientácie: na bok a príliš blízko laptopu (alebo desktopu). V tejto polohe smeruje elektromagnetické vlnenie takmer priamo hore a dole! Nielen, že to vedie polovicu Vášho signálu do stola, rádio je náchylné interferovať so samotným počítačom.

Jedna výnimka zo zmieňovaných záležitostí, ktorá stojí za zmienku, je vstavaná AirPort karta od Apple. Má zabudovaný konektor internej antény, ktorá prechádza cez LCD panel. Toto je vynikajúci dizajn s omnoho lepším dosahom, aj keď vylučuje prídanie externej antény. Zdá sa, že IBM je prvý, kto to chce odkukať, pri jeho iSeries ThinkPad-e.

Uvidíte ohromný rozdiel v sile signálu po pripojení a správnej orientácii malej všesmerovej externej antény k Vášmu klientovi. Ktorý spôsob je správny? To závisí na Vašom prostredí. Vyskúšajte všetky možné polohy so zapnutým meračom sily signálu. Ja som svoju položil na vrch monitora, pod stôl, na bok, na stôl za mnou a dokonca prehodil si ju cez plece. Najlepšia orientácia Vašej antény je vždy v tej polohe, kedy prijíma najlepší signál, preto sa nebojte popohybovať s anténou.

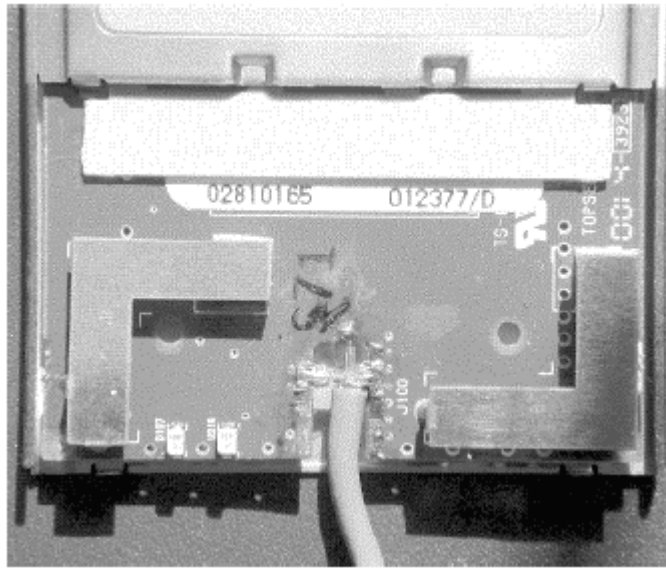
Ak ste v situácii bez externej antény, môžete objavovať krásy RF spustením merača sily signálu a naklopením laptopu na bok. Pozorujte ako graf signálu rastie. Naučte sa písať bokom! Ešte lepšie, prepracujte Vašu sieť tak, aby ste zväčšili dosah a vždy pribaľte rezervnú externú anténu.

Predtým, než sa pozriete, ako pridať antény do Vašej siete, uistite sa, že Vaša karta dokáže pripojiť externú anténu. Veľa lacnejších kariet neobsahuje konektory pre externé antény. Budete mať ťažkosti nájsť správny konektor, pretože každý výrobca ponúka jeho vlastný komerčný konektor (viď [obrázok 6-6](#)). Konzultujte s miestnym rádio dodávateľom, či existuje redukcia z komerčného na štandardný, aj keď sú obyčajne predražené.



Obrázok 6-6. Vykričaný adaptér Lucent Pigtail, cena 80 USD.

Samozrejme, ak máte dobré náradie a dostatok zručnosti pri spájkovaní, môžete mať šťastie vyrobiť si Váš vlastný adaptér, podobný tomu na [obrázku 6-7](#). Prečo minúť 80 USD na hlúpy komerčný konektor, keď si môžete vyrobiť vlastný za pár minút?



Obrázok 6-7. Adaptér typu urob si sám: 3 USD.

Takýto prístup je naozaj praktický len pre pevné, bod-bod spoje, kde nie sú žiadne prekážky na trase. Ako čas beží, množstevné zľavy na pigtail-y z komerčného konektora na štandardný sú čoraz bežnejšie. Nemali by ste zaplatiť viac ako 20-30 USD na adaptér, ak môžete nakupovať vo veľkom od tretej strany. Nezabudnite kúpiť najkratší možný kábel, ktorý dokážete použiť, aby ste minimalizovali stratu signálu v kábli (viď diskusia nižšie v tejto kapitole o výbere kábla).

Pigtail-y sú špecifické od výrobcu (a dokonca čísla modelu), preto sa presvedčte, že beriete správny pigtail pre kartu s ktorou ho plánujete používať. Tiež pretože PCMCIA karty majú obmedzený priestor pre konektory, zástrčka pigtail-u býva *veľmi* jemná. Jedno poriadne trhnutie zničí Váš pigtail, konektor, alebo oba. Boli ste varovaní! (Nie tak ako ja, keď som nevedel ako ľahko sa môžu zlomiť. Dokonca o 2 hod. ráno po príliš veľa espressách a príliš veľa hodinách strávených pri obrazovke, pokúšajúci sa to dokončiť. Nie.)

Hoci pripájate anténu k Vášmu rádiu, vždy nájdite spôsob ako umiestniť Vaše zariadenie tak, aby videlo anténu na druhom konci. Tomu sa hovorí mať priamu viditeľnosť - *line of sight (LOS)* - na ďalší uzol. Zatiaľ čo to len pomáha na kratších spojoch (ako je z Vášho laptopu ku AP), je to úplne nevyhnutné pri bod-bod spojoch na dlhé vzdialenosti. Ideálna trasa by mala byť medzi dvoma anténami, ktoré sú umiestnené na vežiach, poriadne nad akýmkoľvek zemskými odrazmi, s údolím medzi nimi, namierenými priamo jedna na druhú. To je v každom prípade ťažké, ale pokúste sa priblížiť k tomuto ideálu, ako je to len možné.

Pre vonkajšie aplikácie, stromy asi budú Váš najväčší zabijak signálu (nasledované kovom, vlhkým murivom a inými 2.4GHz zariadeniami). Keď vyberáte miesto pre Vašu anténu, zvažujte ako zmeny prostredie ovplyvnia Váš spoj (čo vyzerá ako výborné miesto v zime, môže byť úplne nevhodné na jar kvôli listom). Poprechádzajte sa po dostupnom okolí a pokúste sa nájsť najlepšie možné miesto pre anténu. Nedomnievajte sa, že len najvyšší bod je to miesto na nainštalovanie. Po vyskúšaní všetkých kútov na mojej streche (zbytočne), aby som našiel priamu viditeľnosť na O'Reilly, zišiel som dole a sadol si frustrovaný na moju prednú verandu. Vtedy som si všimol, že vidím danú budovu

vzdialenú pol míle a medzi ňou nič nie je. Postavil som anténu na trojnožku na moju verandu a okamžite som dostal slušný signál. Ponaučenie: správne miesto pre Vašu anténu je iné pre každú inštaláciu.

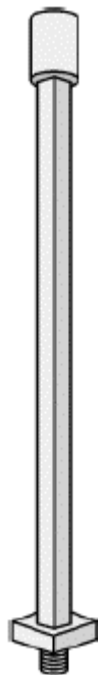
6.2.1 Antény

Antény Vám *nedajú* viac signálu ako je na začiatku (na to sú zosilňovače). Ich úlohou je sústrediť dostupný signál v danom smere, podobne ako pri otáčaní hlavicou baterky. Ona nerobí žiarovku nijak žiarivejšou, len sústreďuje to čo máte do úzkeho priestoru. Zaostrenie baterky má za následok žiarivejší lúč, ktorý pokrýva celkovo menšiu plochu a obdobne, väčšími smerové antény dávajú silnejší, zrozumiteľnejší signál v menšom priestore. Všetky antény sú tak trochu smerové, a miera ich smerovosti je označovaná ako *zisk* - *gain*. Obvykle, čím vyšší je zisk, tým väčší je dosah (najlepší je v smere, ktorým anténa vyžaruje).

Sú štyri rôzne základné druhy antén vhodné pre použitie pri 2.4GHz. Každá funguje dobre pre svoj účel, a žiadna samostatná anténa nefunguje najlepšie pre všetky účely. Naplánujte si vopred čo je Vaším cieľom a nastavte Vašu sieť tak, aby ste to dosiahli. Nasledujúce odseky popisujú najbežnejšie druhy antén, zoradené zhruba podľa smerovosti.

6.2.1.1 Všesmerovka - Omni

Všesmerová anténa (alebo omni) znázornená na [obrázku 6–8](#), vyžaruje vo všetkých horizontálnych smeroch zhruba rovnako. Predstavte si rozloženie obrovského prstenca okolo stredu stožiara všesmerovky. Takto vyzerá elektromagnetické žiarenie. Je to vhodné na pokrytie veľkej plochy, keď nevíete z ktorého smeru môžu prísť Vaši klienti. Nevýhodou je, že aj šum prijímajú zo všetkých smerov, preto obvykle nie sú natoľko efektívne ako smerovejšie antény.



Obrázok 6–8. Všesmerovky sú od drobných nastavcov, po stožiare umiestnené na budovách

Vyzerajú ako vysoké, tenké stožiare, od jednej do päť stôp dlhé, a bývajú drahé. Čím sú dlhšie, tým viac elementov obsahujú (a obvyčajne majú väčší zisk a vyššiu cenu).

Upevňujú sa vertikálne, podobne ako cencúľ. Získavajú v horizontálnom smere na úkor vertikálneho. To znamená, že najhoršie miesto pre spojenie sa so všesmerovkou je presne pod (alebo nad) ňou. Vertikálna citlivosť sa prudko zlepšuje s narastajúcou vzdialenosťou od antény.

6.2.1.2 Sektorová

Predstavte si všesmerovku so zrkadlom za ňou a dostanete obraz elektromagnetického žiarenia sektorovej antény. Sektorka vyžaruje v jednom smere, s lúčom širokým 180 stupňov, alebo úzkym 60 stupňov (alebo dokonca menej). Vynikajú pri bod-multibod aplikáciách, kedy niekoľko klientov pristupuje k bezdrôtovej sieti z toho istého smeru.

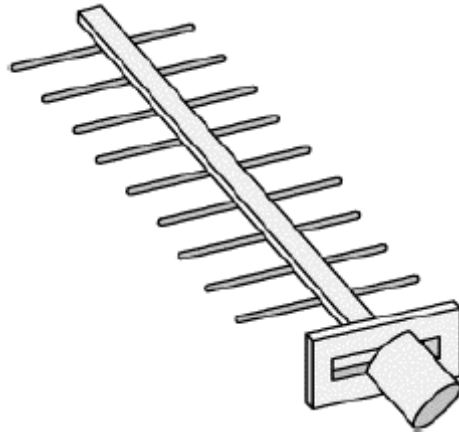
Sektorové antény (znázornená na *obrázku 6–9*) sa vyskytujú v rôznom prevedení, od sploštených všesmeroviek (vysoké, tenké a obdĺžnikové) po malé, ploché štvorce, alebo kruhy. Niektoré majú len osem palcov naprieč a upevňujú sa na plocho oproti zvislej stene, alebo otočne. Tiež sa môžu upevňovať na strop, aby poskytli prístup v jednej miestnosti, ako je rokovacia miestnosť, školská trieda, alebo podlažie výstavniska. Tak ako pri všesmerovkách, cena je obvykle úmerná zisku.



Obrázok 6–9. Sektorové antény bývajú ploché a tenké.

6.2.1.3 Yagi

Yagi vyzerajú ako staré televízne antény. Je to buď plochý kus kovu s radom priečných horizontálnych kúskov, alebo dlhá rúrka s radom podložiek pozdĺž nej (viď *obrázok 6–10*). Obvykle sa lúč môže pohybovať od 15 stupňov až po 60, záleží na type antény. Tak ako pri všesmerovke, pridávanie viacerých elementov znamená väčší zisk, dlhšiu anténu a vyššiu cenu.



Obrázok 6–10. Yagi sa vyskytuje v rôznych tvaroch, ale všetky majú násobné elementy.

Niektoré Yagi sú jednoducho holé, ako ploský vianočný stromček, namierený približne v smere komunikácie. Iné sú vsadené v dlhých, horizontálnych PVC púzdрах. Fungujú dobre pri bod-bod, alebo bod-multibod aplikáciách a obvykle dosahujú vyšší zisk než sektorové.

6.2.1.4 Parabolický tanier

V určitom smere je tanier opakom ku všesmerovke. Namiesto pokúšania sa pokryť celú oblasť, tanier sa zameriava na veľmi úzky priestor (viď [obrázok 6–11](#)). Taniere majú obvykle najvyšší zisk a najväčšiu smerovosť zo všetkých antén. Sú ideálne pre spoje bod-bod a takmer nepoužiteľné pre všetko ostatné.



Obrázok 6–11. 24dB parabolický tanier.

Taniere môžu byť plné, alebo sieťované, malé 18 palcov naprieč, alebo veľké ako chcete (30 stopový tanier je možný, ale asi nie veľmi bežný). Tanier, ktorý dokáže poslať 802.11b signál na viac než 20 míľ, môže mať rozmery niekoľkých stôp naprieč. Ak porovnávame pomer cena/zisk, taniere sú snáď najlacnejšie typy antén. Niektorí ľudia si úspešne prerobili staré satelitné a DSS taniere na 2.4GHz taniere, viď odkazy v [prílohe A](#).

Jedna z ďalších charakteristík antén, ktorá stojí za zmienku, je *polarizácia*. Polarizácia antény znamená smer, ktorým vstupujú elektrické častice elektromagnetického vlnenia. Obe, horizontálna aj vertikálna polarizácia sú bežné, ale v niektorých exotických anténach je možná kruhová (v smere, alebo proti smeru hodinových ručičiek) polarizácia. Polarizácia antény na každom konci spoja musí súhlasiť, inak budú mať rádiá problém spolu komunikovať. Všesmerovky a sektorové majú vertikálnu polarizáciu. Yagi a taniere môžu byť montované vertikálne, alebo horizontálne, záleží na aplikácii. Pri spoji bod-bod vyskúšajte obe a uvidíte pri ktorej je menej šumu. Polarizácia taniera je určená polohou prijímacieho elementu, nie predného reflektora (preto oválny tanier, ktorý chodí hore a dolu, je pravdepodobne montovaný s horizontálnou polarizáciou a preto nebude schopný veľmi dobre komunikovať so všesmerovkou).

Tiež môžete využiť polarizáciu vo svoj prospech. Napríklad, môžete používať dva paralelné spoje na tom istom kanály, jeden s vertikálnou a jeden s horizontálnou polarizáciou. Ak sú vzdialené pár stôp, môžu dva taniere pracovať celkom šťastne na tom istom kanály, bez vzájomnej interferencie, poskytujúc dvojnásobnú šírku pásma na tej istej frekvencii. Toto usporiadanie by požadovalo štyri antény, štyri rádia a prepojovací Ethernetový kanál na každom konci, ale je úplne reálne.

6.2.1.5 Káble

Nie všetky koaxiálne káble sú vhodné pre 2.4GHz použitie. Ten istý kus kábla, ktorý prenáša vysoko kvalitné video a audio do Vášho televízora, je takmer nepoužiteľný pre pripojenie mikrovlnnej antény. Výber správneho typu a dĺžky kábla, je rovnako dôležitý, ako výber správnej antény. 12dB sektorová anténa je nanič, ak stratíte 18dB v kábli, ktorý ju pripája k rádiu. Aj keď každý kábel predpokladá nejakú stratu, keď ním signál prechádza, niektoré typy káblov sú pre 2.4GHz lepšie ako iné.

LMR je druh koaxiálneho kábla, vyrobeného firmou Times Microwave Systems (<http://www.timesmicrowave.com/>) a je to snáď najpopulárnejší typ kábla používaného pre rozrastajúce sa 802.11b siete. LMR používa pletené vonkajšie tienenie a pevný stredový vodič a je k dostaniu v rozličných veľkostiach.

Heliac je ďalší druh mikrovlnného kábla, vyrobeného firmou Andrew Corporation (<http://www.andrew.som/>). Skladá sa z polotuhého zvlneného vonkajšieho tienenia (druh ohybnej medenej trubice), miesto pletených prameňov nachádzajúcich sa v koaxiále. Stredový vodič môže byť buď pevný, alebo zvlnená vnútorná trubica. Je navrhnutý prenášať omnoho vyššie zaťaženie než (legálne) 802.11b inštalácie, ale je veľmi drahý a je obtiažné s ním pracovať. Má tiež extrémne nízku stratu. Označenie druhu dielektrika začína na LDF¹¹.

Okrem ponúk od Times Microwave a Andrew, spoločnosť Belden Inc. (<http://www.belden.com/>) tiež vyrobila veľmi bežný kus kábla, ktorý pracuje dobre v rozsahu 2.4GHz. Často uvidíte odkazy na 9913, to znamená Belden 9913.

¹¹ Nezačínajte si so vzduchovým dielektrikom. Kábel so vzduchovým dielektrikom na výkonovej úrovni 802.11b, to je ako ísť s povestnou sloňou puškou na komára.

Obecne povedané, čím hrubší a lepšie stavaný kábel, tým nižšia strata a vyššia cena (viď [tabuľka 6-1](#)). S káblom presahujúcim hrúbku okolo pol palca je obtiažné pracovať a môže byť ťažké nájsť preň konektor. Kedykoľvek je to možné, objednajte si presnú dĺžku, ktorú potrebujete, s už pripevnenými správnymi konektormi, namiesto pokúšania sa rezať a lemováť to svojpomocne. Komerčný obchod obvykle bude mať potrebné náradie a skúsenosti na výrobu dobre stavaného kábla. Najlepší kábel na svete Vám nepomôže, ak nemáte správne pripevnený konektor.

Tabuľka 6-1. Útlm, veľkosť a približná cena mikrovlnného koaxiálu.

Typ kábla	Priemer	Strata v dB/100' pri 2500MHz	približná cena za stopu
LMR-200	0.195"	16.9	0.37 USD
LMR-400	0.405"	6.8	0.64 USD
LMR-600	0.509"	4.4	1.30 USD
LMR-900	0.870"	3.0	3.70 USD
LMR-1200	1.200"	2.3	5.50 USD
Belden 9913	0.405"	8.2	0.97 USD
LDF1-50	0.250"	6.1	1.66 USD
LDF4-50A	0.500"	3.9	3.91 USD
LDF5-50A	0.875"	2.3	2.27 USD
LDF6-50	1.250"	1.7	10.94 USD
LDF7-50A	1.625"	1.4	15.76 USD

Zhrnutie: použite najkvalitnejší kábel, aký si môžete dovoliť, s najkratšou možnou dĺžkou. Pár dB sem a tam sa skutočne sčítava. Ak chcete umiestniť anténu na strechu, poobzerajte sa po vodotesnom púzdre pre Váš router a umiestnite ho tak blízko ku anténe, ako je to len možné. Potom natiahnite Váš Ethernetový kábel, tak ďaleko, ako potrebujete (do 100 metrov!).

6.2.2 Konektory

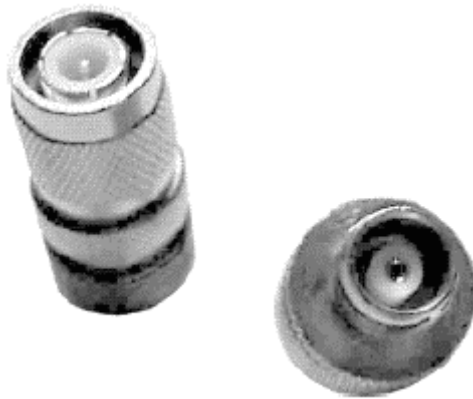
Už máte rádio, anténu a potrebnú dĺžku kábla. Ako ich spojiť dohromady? Potrebujete použiť konektory, ktoré dobre fungujú v pásme 2.4GHz, prispôbiť typ kábla, ktorý používate a navzájom ich spojiť. Prakticky všetky bežné konektory majú dve polovice, samca a samicu (alebo kolík a zdierku). Zopár väčšmi exotických druhov (ako APC-7) je bezpohlavných, takže hociktorý konektor sa môže spojiť s hociktorým. Tu sú najbežnejšie konektory, na ktoré môžete pravdepodobne naraziť.

Bayonet Navy Connector (BNC) je malý, lacný konektor používajúci rýchlo-spojenie polovičným otočením (rovnaký konektor nájdete na 10base2 Ethernete). BNC (zobrazený na [obrázku 6-12](#)) nie je dobre prispôbený pre 2.4GHz použitie, ale je tu zmienený, pretože so zánikom 10base2 sú konektory často predávané lacno. Nedajte sa zlákať.



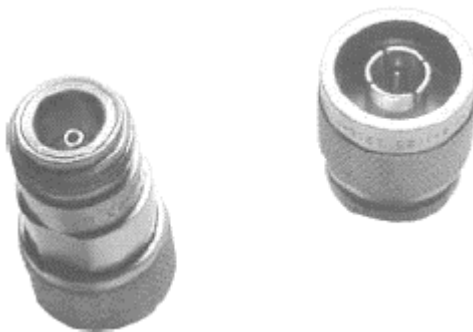
Obrázok 6-12. BNC: Bayonet Navy Connector (alebo Bayonet Neill Concelman, záleží na tom koho sa opýtate).

TNC (viď [obrázok 6-13](#)) je závitová (threaded) verzia BNC. Presný závit pomáha eliminovať rozptyl pri mikrovlnnej frekvencii. TNC fungujú spoľahlivo až po 12GHz a sú často používané s menšími (a viac stratovými) káblami.



Obrázok 6-13. TNC (závitové BNC).

N konektor („Navy“, alebo „Neill“) je väčší, závitový konektor nachádzajúci sa v mnohých komerčných 2.4GHz anténach (viď [obrázok 6-14](#)). Je omnoho väčší než TNC. Funguje veľmi dobre na hrubších kábloch (ako LMR-400) a pracuje dobre až po 10GHz. N je snáď najbežnejšie sa vyskytujúci konektor dodávaný s 802.11b kompatibilnými zariadeniami.



Obrázok 6-14. N konektor.

Takzvaný UHF konektor vyzerá ako hrubo-závitová verzia N (viď [obrázok 6-15](#)). Nie je použiteľný pre 2.4GHz, ale často si ho mýlia s N. Podľa ARRL mikrovlnného manuálu je to PL-259 (ktorý pasuje do zdierky SO-239). Nie je navrhnutý pre prácu na mikrovlnnej frekvencii. Mali by ste sa mu vyhnúť.



Obrázok 6-15. Takzvaný "UHF" konektor.

SMA konektor ([obrázok 6-16](#)) je veľmi populárny, malý, závitový konektor, ktorý pracuje skvelo do 18GHz. Jeho malá veľkosť neumožňuje použitie s väčšími, menej stratovými káblami.



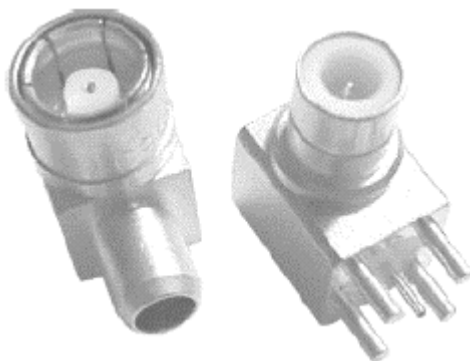
Obrázok 6-16. SMA: Sub-Miniature konektor, typ A.

SMB ([obrázok 6-17](#)) je rýchlo-spájacia verzia SMC.



Obrázok 6-17. SMB: Sub-Miniature konektor, typ B.

SMC (viď [obrázok 6-18](#)) je veľmi malá verzia SMA. Je dobrý do 10GHz, ale je použiteľný len s veľmi malými (vysoko stratovými) káblami. Keby ho rádio výrobcovia štandardizovali ako vyvolený konektor pre externé antény, nebola by žiadna potreba redukčných pigtail-ov.



Obrázok 6-18. SMC: Sub-Miniature konektor, typ C.

APC-7 ([obrázok 6-19](#)) je 7mm, bezpohlavný konektor, použiteľný do 18GHz. Je to vysoko kvalitný konektor, vyrobený firmou Amphenol a je drahý, veľmi zriedkavý a s nízkou stratou.



Obrázok 6-19. APC-7: presný konektor Amphenol.

Pamätajte na to, že každý konektor v systéme spôsobuje nejaké straty. Vyhýbajte sa redukciám a nie nevyhnutným konektorom všade, kde sa to dá. Taktiež, profesionálne vyrábané káble bývajú kvalitnejšie, ako káble, ktoré zakončíte sami (ak nie ste naozaj dobrý a nemáte to správne náradie). Vždy, keď je to možné, pokúste sa kúpiť predpripravený kábel s už pripojenými správnymi konektormi, najkratšej použiteľnej dĺžky. 802.11b zariadenia nemajú veľký výkon a tak každá troška pomôže rozšíriť Váš dosah a spoľahlivosť. Je jednoduché vyrobiť zlý kábel a zlý kábel môže zapríčiniť nekončiace problémy.

Keď spájate káble s Vaším zariadením, môžete naraziť na konektor opačného pohlavia (samec a samica prehodené, s rovnakým závitom), s opačným závitom (ľavý namiesto pravého závit), alebo dokonca opačné pohlavie s opačným závitom (obidva). Presvedčte sa, že viete čo beriete, predtým než si objednáte súčiastky online!

Pre vonkajšie použitie je náležitá ochrana proti bleskom životne dôležitá. Plynová trubica zachytávajúca blesky (viď [obrázok 6-20](#)) dokáže poskytnúť vysoký stupeň ochrany (oba, pre Vaše zariadenia, aj proti požiaru) pred údermi bleskom do Vašej antény.



Obrázok 6-20. Plynová trubica zachytávajúca blesky.

Má cenu niekde medzi 30-100 USD a ak je správne inštalovaná, dokáže poskytnúť ochranu pred viacnásobnými údermi bleskom. Určite si naštudujte správnu inštaláciu, použite kvalitné uzemnenie a ak máte pochybnosti, obráťte sa na profesionálov. Veľa bleskoistiek, ktoré som videl, mali samicu N konektora na oboch koncoch, preto to nezapodnute zohľadniť, keď plánujete Vašu hardvérovú inštaláciu.

6.2.3 Výpočet dosahu

Ako ďaleko sa Váš signál dostane? To je veľmi dobrá otázka. To závisí na všetkých druhoch faktorov, vrátane výstupného výkonu a citlivosti Vašej karty, kvality Vášho kábla, konektorov a antény, vyskytujúceho sa rušenia a šumu a dokonca od počasia (pri dlhých spojoch). Aj keď je nemožné vziať všetky tieto premenné správne do úvahy, môžete si urobiť dobrý, približný výpočet predtým, než kúpite akýkoľvek hardvér. Tu je

jednoduchý spôsob ako zostaviť približný výpočet (často označovaný ako Váš *rozpočet spoja – link budget*).

Najskôr zistíte, aká je strata signálu v priestore, medzi danými dvoma miestami. To sa nazýva *strata cestou – path loss*. Jeden zo zaužívaných vzorcov na odhad tejto straty pri 2.4GHz je:

$$L = 20 \log(d) + 20 \log(f) + 36.6$$

pričom L je strata v dB, d je vzdialenosť v míľach a f je frekvencia v megahertzoch.

Predpokladajme, že chcete vytvoriť spoj na päť míľ, medzi dvoma bodmi, pri použití kanála 6 (2.437GHz):

$$L = 20\log(5) + 20\log(2437) + 36.6$$

$$L = (20 \times 0.69) + (20 \times 3.38) + 36.6$$

$$L = 13.8 + 67.6 + 36.6$$

$$L = 118$$

Na piatich míľach, bez prekážok, stratíte 118dB zo signálu medzi dvoma bodmi. Náš spoj musí dovoliť takúto veľkú stratu (plus trochu navyše pre zohľadnenie poveternostných vplyvov a rôznych interferencií), inak bude nespoľahlivý.

Ďalej pridajte všetky Vaše zariadenia (rádiá + antény + zosilňovače) a odpočítajte Vaše straty (dĺžka kábla, konektory, bleskoistky a rôzne ďalšie straty). Predstavme si, že používate karty Orinoco Silver (15dBm), žiadne zosilňovače, 12dBi sektorovú anténu na jednej strane a 15dBi Yagi na druhej. Ďalej povedzme používate jeden meter LMR-400 a bleskoistku na každej strane, pripusťme 0.25dB stratu v každom konektore a 1dB na každý pigtail. Nakoľko sú všetky jednotky v dB, môžeme použiť jednoduché sčítanie a odpočítanie:

rádio - pigtail - bleskoistka - konektor - kábel - konektor + anténa

$$\text{strana A: } 15 - 1 - 1.25 - 0.25 - 0.22 - 0.25 + 12 = 24.03$$

$$\text{strana B: } 15 - 1 - 1.25 - 0.25 - 0.22 - 0.25 + 15 = 27.03$$

$$A + B = 51.06 \text{ celkový zisk}$$

Teraz odpočítajme stratu cestou od celkového zisku:

$$51.06 - 118 = -66.94$$

To to je úroveň signálu vnímaná na oboch koncoch spoja: -66.94dBm. Ale je to dostatočné na komunikáciu?

Po vyhľadání špecifikácie citlivostí prijímača pre kartu Orinoco Silver (musíte ju hľadať, ale nachádza sa v manuáli) nájdeme výsledok uvedený v [tabuľke 6-2](#).

Tabuľka 6-2. Matica citlivostí prijímača pre kartu Orinoco Silver.

11Mbps	5.5Mbps	2Mbps	1Mbps
-82dBm	-87dBm	-91dBm	-94dBm

Pretože generujeme signál -66.94dBm máme „zálohu“ 15.06dB ($82 - 66.94 = 15.06$). Teoreticky, zvyčajne to bude fungovať pri 11Mbps (za dobrého počasia) a nemalo by to mať žiadne problémy pri synchronizácii na 5.5Mbps. Rádia by mali automaticky detekovať, keď sa spojenie stáva nespoľahlivé a presynchronizovať sa na najvyššiu dosiahnuteľnú rýchlosť.

Obyčajne, pásmo pre chyby okolo 20dB je dostatočné, aby vykrylo normálne poveternostné vplyvy. Použitie výkonnejších rádii (ako je Cisco 350 s 20dBm), alebo väčšími ziskovými anténami, by malo napomôcť spojeniu pri 11Mbps. Pri použití kariet s vyšším ziskom (ako sú karty Cisco, alebo Teletronics) v kombinácii s vysoko ziskovým tanierom je možné rozšíriť Váš dosah nad dobrých 25 míľ.

Online nástroje, ako Green Bay Professional Packet Radio's Wireless Network Link Analysis, Vám môžu podať približný odhad, čo bude potrebné, aby ste zrealizovali Váš spoj, jednoducho len vyplníte pár kolóniek na web formulári. Pozrite si ich vynikajúce zdroje na <http://www.qsl.net/n9zia/wireless/page09.html>.

6.3 Zosilňovače a zákony

Často, keď ľudia premýšľajú o rozšírení dosahu, hneď myslia na použitie zosilňovačov (domnievam sa, že je to prirodzené, máte zosilňovač pre Vaše domáce stereo, prečo nemať zosilňovač pre Vašu sieť?). Dobré zosilňovače, ktoré pracujú v mikrovlnnom pásme, musia prekonať niekoľko netriviálnych technických prekážok:

- Zosilňovače slepo zosilňujú všetko čo majú naladené, signál aj šum. Silnejší signál Vám nepomôže, ak rovnako narastie aj šum v pásme, pretože signál sa jednoducho stratí (ako keď kričíte na svojich kamarátov na koncerte).
- 802.11b rádiová komunikácia je pol duplexná, buď sa vysiela, alebo prijíma, ale nikdy oboje súčasne. Zosilňovač, pripojený ku Vašej anténe, bude musieť automaticky detekovať kedy rádio vysiela a rýchlo zapnúť zosilňovanie. Keď skončí, musí to zase rýchlo vypnúť. Každé oneskorenie pri tomto prepínaní môže v skutočnosti oslabiť komunikáciu, alebo, čo je horšie, zničiť rádiovú kartu.
- Zosilňovač môže trochu pomôcť na strane prijímača pridaním určitého dôrazu, ale v skutočnosti je určený pre vysielanie. To znamená, že ak máte zosilňovač len na jednom konci spoja, druhý koniec Vás môže počuť, ale Vy nemusíte počuť jeho. Aby bolo zosilnenie účinné, potrebujete zosilňovač na oboch koncoch spoja.
- Všetky zosilňovače potrebujú pre svoju činnosť napájanie. To znamená pridanie DC injektora ku napájacíemu káblu antény, alebo použitie externého adaptéra. To v budúcnosti zvýši náklady Vášho uzla a je to ďalšie zariadenie ktorému musíte poskytnúť napájanie.

Záver, zosilňovače, ktoré dobre fungujú s 802.11b zariadeniami, sú drahé (400 USD a viac) a je ich ťažké získať. Ale skutočne ich potrebujete? S použitím štandardných zariadení a vysoko ziskových antén dokázate predĺžiť bod-bod spoj na viac ako 25 míľ, bez použitia zosilňovačov. Vaše peniaze budú snáď lepšie použité na vysoko kvalitné smerové antény a káble a prípadne dokonca pridanie ďalšieho uzla v budúcnosti.

Čo sa týka federálneho práva USA, budete si musieť prečítať Part 15 (viď [príloha A](#)) a urobiť si vlastné závery. Najmite si právnik, ak ste naozaj paranoický. Tim Pozar (BAWUG) vypracoval zopár zaujímavých poznámok týkajúcich sa pravidiel Part 15 vo vzťahu k 2.4GHz emisiám, pozrite si online jeho komentár na http://www.lns.com/papers/FCCPart15_and_the_ISM_2.4G_Band.index.

V krátkosti, množstvo legálne vyžiarého výkonu (a zisk Vašej antény) je limitované, a závisí na tom, ako ho používate. Pevné bod-bod spoje majú pridelený vyšší výkon, zatiaľ čo všesmerové bod-multibod usporiadania sú najviac obmedzené. Ak nepoužívate zosilňovače, pravdepodobne by ste nemali prekročiť limity FCC, pretože štandardné klientské karty nevysielajú tak vysoký výkon. Ale neberte ma za slovo, pretože ja nie som právnik (okrem toho, osoba zodpovedná za to, že Vaše vybavenie je určite legálne, ste Vy, operátor!).

Skutočne verím, že účelom týchto pravidiel je obmedziť interferenciu v pásme, čo je niečo, za čo by sme mali všetci bojovať. Šum je nepriateľ každého. Na koniec, pokúste sa používať minimálne množstvo výkonu, nevyhnutného na to, aby ste udržali spoj funkčný a používajte čo najsmerovjšie antény, ktoré budú vyhovovať Vašej aplikácii. Buďte dobrý sused a snáď zistíte, že Vás susedstvo teší viac.

Kapitola 7. Ďalšie aplikácie

Vďaka úsiliu nespočetného množstva inžinierov máme otvorený 802.11b štandard. Teraz, keď je hardvér, ktorý dodržiava tento štandard, v rukách neinžinierov, všetky druhy zaujímavých aplikácií boli realizované. Tisíce po celej Zemi posúvajú schopnosti týchto nedrahých rádii ďaleko za hranice pôvodne plánovaných možností. Bežná klientská PCMCIA karta bola použitá na vytvorenie chrbticového spoja bod-bod, dlhého niekoľko míľ. Nespokojný s drobnými, súkromnými sieťami, používajú ľudia nedrahé AP na vytvorenie verejných sietí, ktoré sú schopné podporovať stovky užívateľov naraz. Dokonca vykričané bezpečnostné nedostatky 802.11b boli prekonané starostlivým plánovaním a vhodným aplikovaním open source softvéru. Či výbor IEEE zamýšľal, aby tomu tak bolo, alebo nie, 802.11b objavila čarovnú formulkú, ktorá vytvára vrcholnú platformu pre hardvérových hackerov: nízka cena, jednoduchosť používania, ľahká modifikácia a všadeprítomnosť.

V tejto kapitole sa zameriame na niektoré bezdrôtové aplikácie, ktoré demonštrujú enormnú flexibilitu bezdrôtovosti (a niektoré čo sú jednoducho cool!). Upozorňujem, že niektoré z príkladov v tejto kapitole určite spôsobia stratu záruky a môžu zničiť Vaše zariadenie, ak nie ste dosť opatrný. Ak si nie ste istí ako niečo uskutočniť, popýtajte sa. Šance sú, niekto iný už urobil to o čom Vy uvažujete a môže Vám prinajmenšom poskytnúť svoje skúsenosti. Rôzne bezdrôtové diskusné skupiny sú skvelý zdroj pre predstavy a riešenie detailov implementácie.

7.1 Spoj bod-bod

Z pohľadu rádia je spoj bod-bod veľmi jednoznačný na nastavenie. Mali by ste vždy postupovať, viacmenej, podľa rovnakých krokov, keď posudzujete reálnosť spoja:

- Presvedčte sa, že máte priamu viditeľnosť z jedného konca na druhý.
- Zmerajte vzdialenosť medzi danými bodmi a vyrátajte stratu cestou.
- Prirátajte schopnosti Vašich zariadení, aby ste stanovili Váš rozpočet spoja.
- Chodte vonku a zaveste Vaše zariadenie.

Ak plánujete urobiť spoj bod-bod na dlhú vzdialenosť, najskôr si zistíte zemepisnú šírku, dĺžku a nadmorskú výšku každého koncového bodu. Môžete to zistiť fyzicky, pridete na každé miesto a zaznačíte si súradnice pomocou GPS, alebo to môžete odhadnúť použitím topografickej mapy, alebo softvéru (v kapitole 6 nájdete nejaké príklady, ako to urobiť). Pomocou súradníc a nadmorskej výšky oboch miest môžete vypočítať azimut a uhol náklonu, takže zhruba viete kam nasmerovať antény na každom

konci. Poriadne GPS Vám tu môže pomôcť udaním azimutu na a od každého bodu. Tiež by ste si mali pozrieť online bezdrôtový návrh od CGI na: <http://www.qsl.net/n9zia/wireless/page09.html>, ktorý Vám pomôže s viacerými výpočtami, ktoré budete potrebovať uskutočniť.

Samozrejme, ak vidíte druhý bod cez ďalekohľad, alebo teleskop, je to dobrý prvý krok. Najlepšie by bolo, keby na zemi, medzi danými dvoma bodmi, bolo toho čo najmenej. Čím viac sa trasa priblíži ku skutočnému údoliu, tým lepšie. Detaily, ako vypočítať stratu cestou a rozpočet spoja pre Váš spoj, nájdete v [kapitole 6](#). Už som to spomínal, ale znova: nechajte si kábel od antény tak krátky, ako je to len možné! Pri dlhých spojoch bod-bod sa ráta každých pár decibelov.

Teraz ste pripravený zavesiť Vaše zariadenie, zostáva otázka: aké zariadenie chcete použiť? To závisí na Vašom rozpočte a ako plánujete používať daný spoj. Ako sme si ukázali v [kapitole 5](#), je veľmi jednoduché nastaviť Linuxovú bránu v IBSS móde. To je nepochybne najlacnejší spôsob, ako sa dostať z jedného konca na druhý, ale sú s tým spojené nejaké otázky ohľadom smerovania (mnoho bezdrôtových kariet neumožňuje Ethernetové premostenie, preto budete potrebovať použiť maškarádu, aby ste umožnili paketom prechádzať bezdrôtovým spojením). Ak už máte hardvérové AP, môžete ho použiť na jednom konci spoja a klientskú kartu na druhom, s rovnakou konfiguráciou (napr. maškaráda na strane klienta). Nedávno uvedená, lacná hardvérová alternatíva, je AP Linksys WAP-11. Linksys vydal upgrade firmvéru, ktorý umožňuje tomuto AP komunikovať s ostatnými (rovnakými modelmi) vzduchom, buď v bod-bod, alebo bod-multibod móde. Môžete si stiahnuť verziu 1.4f.5 z ich web stránky <http://www.linksys.com/>. Tieto AP stoja približne 200 USD a obsahujú TNC konektor opačného pohlavia pre externú anténu, preto to môže byť nie drahá voľba na vytvorenie spoja bod-bod.

Čím ďalej od seba budú Vaše body, tým ťažšie bude nasmerovať antény. Pri vzdialenostiach zhruba do päť míľ, je to zriedkavý problém (ak máte dostatok celkového zisku, aby ste prekonalí stratu cestou). Pri dlhších vzdialenostiach, nasmerovať antény priamo na seba, môže byť trochu zložité. Tu je niekoľko techník, ktoré Vám snáď pomôžu nasmerovať taniere tam, kam potrebujete:

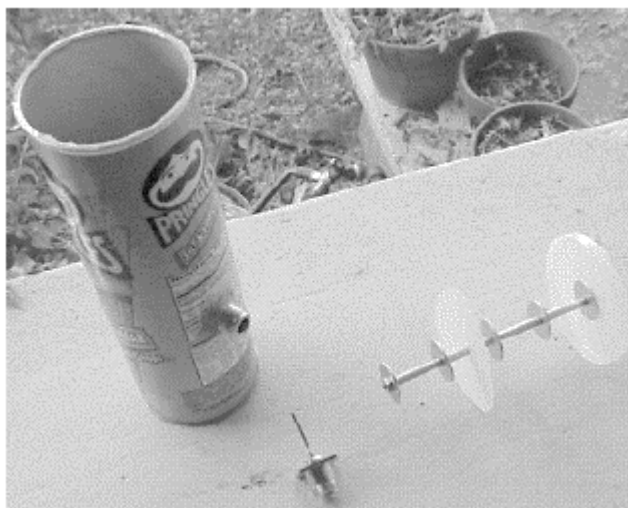
- Použite mobilný telefón, alebo vysielaciu, aby ste mohli komunikovať medzi danými dvoma bodmi, kým smerujete antény. Pomáha, ak máte aspoň dvoch ľudí na každej strane (jeden na manipuláciu s anténou a druhý na koordináciu s druhým koncom).
- Nastavte všetky Vaše sieťové nastavenia vopred, takže už nie sú žiadne nejasnosti, keď sa dostanete na odľahlé miesto. Skontrolujte všetky zariadenia, urobte ping na každý stroj, dokonca preneste jeden, alebo dva súbory, aby ste sa uistili, že Vaše zariadenia fungujú na blízko. Nebudete to musieť preverovať neskôr, ak sa vyskytnú problémy rozchodiť spojenie.
- Použite nástroje ako je Lucent Link Test meter (ktorý sa dodáva spolu s ovládačom pre Windows ku kartám Orinoco) na zobrazenie sily signálu a šumu v reálnom čase. Tento druh nástrojov je Váš najlepší priateľ, niečo ako skutočný spektrálny analyzátor.
- Pracujte len na jednom konci spoja v danom čase, pomaly meňte jednu vec, až kým nedosiahnete maximálnu silu signálu a najnižší šum.
- Ak máte nejakú poruke (a Váš rozpočet spoja to dovoľuje), vyskúšajte najskôr všesmerovku, alebo sektorovú anténu na jednom konci spoja. Keď nájdete druhý koniec spoja, nahraďte ju Vaším tanierom, alebo Yagi a vyladíte ho.

- Pomaly vyladujte a neobávajte sa prejsť za najlepší obdržaný signál. Mnohé antény majú malý postranný výbežok, ktorý zvykne pomýliť. Pohybujte, kým nenájdete hlavný výbežok. Keď už ho nájdete, mal by sa značne líšiť od ostatných.
- Nedotýkajte sa antény pri odčítavaní meraných hodnôt. Ľahko sa to prehliadne keď používate trubicovú Yagi, ako je obal od Pringles (viď nasledujúci odsek). Vaše ruky ponechané na anténnej trubici budú interferovať s elektromagnetickým žiarením a odčerpajú signál veľmi rýchlo. Vykonávajte meranie keď nemáte v rukách žiadne zariadenia.
- Nezabudnite porovnať horizontálnu a vertikálnu polarizáciu. Vyskúšajte antény v oboch pozíciách a použite tú, ktorá vykazuje najnižší šum (viď [odstavce 7.3](#), nižšie v tejto kapitole).
- Keď je Váš spoj funkčný, zvážte použitie WEP na odstránenie ostatných od pokusov pripojiť sa k nemu. Ak chcete poskytovať bezdrôtový prístup na jednom konci, nastavte inú bránu, pokiaľ možno s cache službami (ako je caching DNS a transparent web proxy, napr. Squid). To pomôže znížiť množstvo trafficu, ktorý prechádza spojom, sieťové kolízie a všeobecne omnoho efektívnejšie využiť spoj.

Môže to trvať celý deň, kým správne nastavíte antény na dlhú vzdialenosť, ale so správnou skupinou ľudí, to tiež môže byť zábavné. Jednoducho si nájdite čas, porozmýšľajte čo chcete urobiť a určite si nechajte na konci dňa čas na oslavu!

7.2 Obal od Pringles

Na Portlandskom samite v júni, Andrew Clapp predstavil zvláštny dizajn Yagi antény. Pozostávala zo skrutky, kovovej rúrky, podložiek a PVC trubice, tvoriac nedrahú Yagi, buď 18", alebo 36" dlhú. Aj keď jeho anténa vykazovala zisk medzi 12 a 15dBi (čo je pozoruhodné pre tak jednoduchý dizajn), je trochu veľká. Keď sme sa vrátili z Portlandu, niektorí členovia našej miestnej skupiny aja, sme usúdili, že ak budeme opatrný, dokážeme napasovať celú vlnovú dĺžku vnútri obalu od Pringles, ako je to zobrazené na [obrázku 7-1](#). Malo by to vykazovať menší celkový zisk, ale tiež by to malo urobiť celú anténu omnoho kompaktnejšou.



Obrázok 7-1. Kompletná anténa - je to jednoducho len obal!

7.2.1 Zoznam súčiastok

Tu sú položky, ktoré budete potrebovať pre zostrojenie antény z obalu od Pringles:

Dielec	Približná cena
celozávitový diel, 5 5/8" dĺžka, 1/8" vonkajší priemer	1 USD
dve nylonové poistné matice	0.1 USD
päť 1" podložiek, 1/8" vnútorný priemer	0.1 USD
6" hliníková trubica, 1/4" vnútorný. priemer	0.75 USD
konektor na pripojenie Vášho pigtailu od rádia (my sme použili samicu N konektora)	3 USD
1 1/2" kus pevného medeného drôtu veľkosti 12 (my sme použili uzemňovací drôt z domáceho elektrického rozvodu)	zanedbateľná
vysoký obal od Pringles (hocijaká príchuť, lemovanie je voliteľné)	1.5 USD
plastikový disk z odpadu, 3" naprieč (ako vrchnák z ďalšieho obalu od Pringles)	zanedbateľná
Spolu	6.45 USD

Samozrejme, nakupovanie vo väčšom pomôže. Možno nebudete môcť pozháňať 6 palcový celozávitový kus, kúpte štandardnú veľkosť (obvykle jednu, alebo dve stopy) a balenie po 10 podložiek a matic. Potom budete mať viac ako dosť súčiastok na výrobu dvoch antén, všetko za približne 10 USD.

7.2.2 Potrebne náradie

Budete potrebovať nasledujúce náradie na výrobu Vašej antény:

- pravítko
- nožnice
- pílkou na trubicu
- pílkou na odrezanie celozávitového kusu
- niečo ostré na prederavenie plastiku (niečo ako šidlo)
- teplovzdušnú pištoľ (ak nemáte skrutkovací typ konektora)
- spájkovací kov

Potrebný čas je približne hodina.

7.2.3 Konštrukcia predného kolektora

Označte a odrežte štyri kusy trubice, dlhé približne 1.2 palca (1 15/64 palca). Kde som zobral toto číslo? Najskôr, určite vlnovú dĺžku na spodku frekvenčného rozsahu, ktorý budete používať (2.412GHz, alebo kanál 1). To bude najväčšia dĺžka, ktorú by mala mať trubica:

$$W = 3.0 \times 10^8 \times (1 / 2.412) \times 10^{-9}$$

$$W = (3.0 / 2.412) \times 10^{-1}$$

$$W = 0.124 \text{ metra}$$

$$W = 4.88 \text{ palca}$$

Narežeme rúrku na štvrtiny vlnovej dĺžky, takže:

$$1/4 W = 4.88 / 4$$

$$1/4 W = 1.22 \text{ palca}$$

Teraz určíme, aká je najkratšia dĺžka, ktorú kedy použijeme (2.462GHz, alebo kanál 11 v USA):

$$W = 3.0 \times 10^8 \times (1 / 2.462) \times 10^{-9}$$

$$W = (3.0 / 2.462) \times 10^{-1}$$

$$W = 0.122 \text{ metra}$$

$$W = 4.80 \text{ palca}$$

$$1/4 W = 1.2 \text{ palca}$$

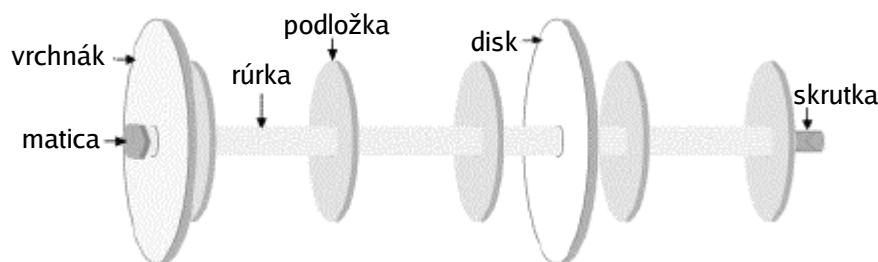
Prakticky, aký je rozdiel medzi najkratšou a najdlhšou rúrkou? Okolo 0.02 palca, alebo menej než $1/32$ palca. To je približne rozmer listu píľky, ktorú používate. Preto jednoducho strelte 1.2 a budete to mať dostatočne presné.

Odrežte celozávitový kus na presne $5 \frac{5}{8}$ palca. Podložky, ktoré použijeme, sú $1/16$ palca hrubé, takže to by nám malo nechať dosť priestoru pre rúrkou, podložky a matice.

Vyrobte otvor v strede vrchnáka od Pringles, dostatočne veľký na to, aby ním prešiel celozávitový kus. Teraz prišiel vhodný čas začať jesť Pringles.

Vystrihnite 3 palcový plastový disk, tak veľký, aby pohodlne zapadol do vnútra obalu. Zistili sme, že vrchnák od ďalšieho Pringles, s orezaným vonkajším lemom, je tak akurát. Zrobte dieru do jeho stredu a navlečte ho na jednu dĺžku rúrky.

Teraz zostavte rúrkou. Môžno budete musieť použiť pilník na obrúsenie konca závit, ak budete mať problém nasadiť naň matice. Rúrka je ako sendvič, ktorý sa navlečie na celozávitový kus, tak ako je znázornené na [obrázku 7-2](#).



Obrázok 7-2. Matica, vrchnák, podložka, rúrkou, podložka, rúrkou, podložka, rúrkou s plastovým diskom, podložka, rúrkou, podložka, matica.

Utiahnite pevne matice, ale nepretočte ich (ja som pri prvom pokuse ohol rúrkou, hliník sa ohne veľmi ľahko). Len aby boli pevné. Gratulujeme, teraz máte predný kolektor, rovnaký ako je na [obrázku 7-2](#).

7.2.4 Príprava obalu

Doteraz by ste už mali mať zjedený Váš kusok. Vytrite obal a namerajte $3 \frac{3}{8}$ palca od spodku obalu. Vyrežte dieru, tak veľkú, aby cez ňu prešiel konektor. Zistili sme, metódou pokus-omyl, že toto sa zdá byť „sweet spot“ obalu. Na našom obale Pringles Salt & Vinegar sadol N konektor priamo medzi „Sodium“ a „Protein“.

7.2.5 Konštrukcia elementu

Vyrovnajzte hrubý medený drôt a prispájajte ho ku konektoru. Keď je vnútri obalu, mal by byť drôt pod stredom obalu (naš mal približne $1 \frac{1}{16}$ palca). Pri dlhšom stratíte pár dB, preto ho odrežte tesne okolo stredu obalu.

My sme sa ponáhľali, preto sme použili teplom vytvrdzovaný lep na upevnenie konektora na miesto pri našej prvej anténe. Ak máte konektor, ktorý používa podložku a maticu a ste skutočne opatrný pri rezaní otvoru, je to tiež dobré riešenie (a nie tak špinavé ako lepidlo). Len si uvedomte, keď pripájate Váš pigtail, že je to zaskrutkované do lepenky. Ľahko sa na to zabúda a môžete nechtiac roztrhnúť stenu obalu.

Teraz zasunúť zostavu kolektora do obalu a uzavrite vrchnák. Vnútorňý koniec rúrky by sa *nemal* dotýkať medeného elementu, mal by byť jednoducho pred ním. Ak sa dotýka, je Váš celozávitový kus asi príliš dlhý. [Obrázok 7-3](#) znázorňuje kompletnú anténu.



Obrázok 7-3. Kompletná anténa.

Ako môže niekto odhadnúť zisk, bez pripojenia ku špičkovému prístroju na analýzu rádii? Pri použití softvéru Link Test, ktorý je dodávaný s kartami Orinoco Silver, môžete snímať signál a šum (v dB) prijímaného signálu a Váš testovací partner príjem Vášho signálu. Keďže som býval 0.6 mile (s priamou viditeľnosťou) od riaditeľstva O'Reilly, mali sme možnosť s tým experimentovať. Použili sme všesmerovku na streche a AP u O'Reilly ako nášho testovacieho partnera spoja.

Aby sme odhadli charakteristiky antén, začali sme pripojením komerčných antén so známym ziskom a odmerali sme ich. Potom sme pripojili naše testované antény a porovnali výsledky. K dispozícii sme mali nasledovné:

- dve 10dBi, 180 stupňov, sektorové panelové antény
- jednu 11dBi, 120 stupňov, sektorovú panelovú anténu
- jeden 24dBi parabolický tanier
- pár obalov od Pringles a nejaký hardvér

Priemerný prijatý signál a šum od každej, v približne rovnakej fyzickej pozícii:

Anténa	Signál	Šum
10dBi A	-83db	-92db
10dBi B	-83db	-92db
11dBi	-82db	-95db
24dBi	-67db	-102db
obal od Pringles	-81db	-98db

Výsledky signálu testovacieho partnera (strana AP) boli prakticky rovnaké. Čo je zaujímavé, dokonca aj keď len na 0.6 míle, spozorovali sme efekt oslabenia vplyvom tepla, keď sa večer zmenil na noc, spozorovali sme cca. 3dB zisk pri každej anténe. (Bol to obzvlášť horúci deň, takmer 100 stupňov. Nevieť aká bola relatívna vlhkosť, ale zdalo sa byť veľmi sucho.)

Yagi a taniere sú omnoho smerovejšie než sektorové a všesmerovky. Dokazujú to aj čísla, vnímaná úroveň šumu bola stále nižšia pri väčších smerových anténach. To môže hodne pomôcť pri spojoch na dlhé vzdialenosti, pretože nie len že vnímaný signál bude lepší, ale aj šum sa zdá byť menší. Väčšími smerovými anténami tiež pomáhajú udržať šum na nízkych hodnotách voči Vaším susedom, keď sa pokúšate zdieľať spektrum. Buďte dobrý sused a používajte najsmerejšie antény, aké budú fungovať pre Vašu aplikáciu (áno, šum je problém všetkých).

Zdalo sa, že obal od Pringles mal veľký postranný výbežok, ktorý presahoval 45 stupňov od stredu obalu. Nesmerujte obal priamo na miesto kde sa pokúšate dostať, cieľte mierne vľavo, alebo vpravo. Tiež sme spozorovali, že zdvihnutie antény tiež trochu pomáha. Keď mierite anténou, držte ju za konektorom, a *pomaly* presúvajte zľava doprava, so spusteným programom Link Test. Keď dostanete maximálny signál, pomaly zdvihnite koniec obalu, aby ste videli, či sa niečo mení. Robte to pomaly, meňte len jednu premennú v danom čase.

Pamätajte, že obal je polarizovaný, preto sa musíte zhodnúť s fázou antény s ktorou chcete komunikovať. Napríklad, ak používate všesmerovku, presvedčte sa, že element je naspodku, alebo navrchu obalu, inak to nebude fungovať. Pozrite si vyššie diskusiu o polarizácii antén, aby ste získali viac informácií o tom, ako využiť tento efekt vo svoj prospech.

Mali sme šťastie a jeden člen našej komunitnej skupiny priniesol merač vratných strát na jedno z našich stretnutí. Boli sme schopný vykonať nejaké reálne merania, koľko signálu sa vráti do rádia. Výsledky neboli tak dobré, ako som dúfal, ale ukázali, že anténa je použiteľná, obzvlášť pri nižších frekvenciách. Najpravdepodobnejšie sme nevzali správne do úvahy hrúbku podloží a to spôsobilo, že predný element bol trochu prídlhý. Rádio nevysielalo tak veľa signálu, aby sa mohlo poškodiť vplyvom vysokých vratných strát, ale ukázalo to, že anténa nie je tak dobre naladená, ako by mala byť.

Neriešili sme vodotesné uloženie obalu, vloženie celej veci do nejakého 3 palcového PVC by to zrobilo. Pri priamej viditeľnosti s krátkymi anténnymi káblami, by mal byť spoj 12dB obal-12dB obal, schopný preniesť 11Mbps na viac ako desať míľ. Môžete online sledovať náš pokrok s obalom na: <http://nocat.net/>.

7.3 Zdvojené spoje

Všetky antény vykazujú charakteristiku známu ako polarita, čo znamená smer, ktorým sa pohybuje elektrické pole, keď opúšťa anténu. Magnetické vlny opúšťajú anténu súčasne s elektrickými, pričom sú navzájom pod uhlom 90 stupňov. Veľa bežných antén vykazuje lineárnu polaritu (napr.: vertikálnu, alebo horizontálnu). Niektoré antény, ako je vinutá skrutkovicová anténa¹², dokonca demonštrujú kruhovú polarizáciu, kedy vlny vystupujú von v špirále, pričom sú vždy navzájom kolmé.

Keď požadujete, aby jedna anténa bola schopná prijímať signály od druhej, musia sa ich polarity zhodovať. Všesmerovky (a väčšina sektorových) majú vertikálnu polarizáciu. Taniere a Yagi môžu byť montované vertikálne, horizontálne, alebo niekde

¹² Pozrite si detaily a plány tohto zaujímavého dizajnu na <http://users.bigpond.net.au/jhecker/>.

medzi. Obal od Pringles je jednoducho Yagi a jeho polarizácia je určená polohou konektora antény. Polarizácia antény s kruhovou polarizáciou (ako je skrutkovicová) je daná smerom vonkajšieho vinutia: buď v smere, alebo proti smeru hodinových ručičiek.

Polarizáciu môžete využiť vo svoj prospech, aby ste eliminovali nejaký šum pri dlhých spojoch. Najskôr vyskúšajte každý koniec pri vertikálnej polarizácii a zmerajte vnímaný šum. Potom otočte každý koniec o 90 stupňov a zmerajte šum opäť. Použite tú polohu, pri ktorej je najmenšie množstvo šumu a mali by ste mať stabilnejší spoj.

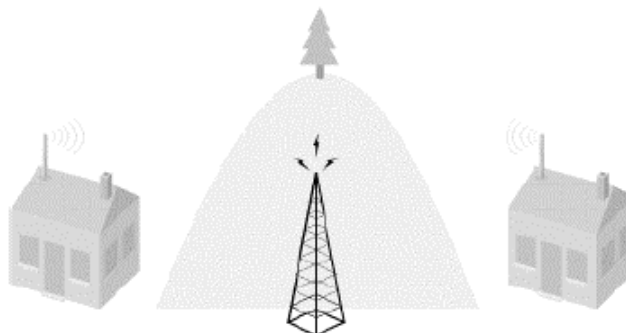
Keďže anténa môže prijímať signály len z antén, ktorých polarizácie sa zhodujú z jej, môžete túto vlastnosť tiež využiť na vytvorenie efektívnejšieho zdvojeného spoja. Napríklad, predpokladajme, že chcete použiť dva rádiá na každom konci spoja, aby ste poskytli celkovú šírku pásma 22Mbps pre odľahlé miesto. Obvykle by ste potrebovali použiť dva kanály, oddelené o 25MHz (napr.: 1 a 6, alebo 2 a 7, alebo 3 a 8). Ak použijete jednu anténu s vertikálnou a druhú s horizontálnou polarizáciou a oddelíte ich o niekoľko stôp, môžete používať ten istý kanál pre všetok Váš traffic. To znamená menší šum v pásme pre Vás samých a aj pre Vašich susedov (a teoreticky Vám to poskytuje 6 možných súbežných spojov, zatiaľ čo normálne sú možné len 3).

Kam až IP siahla, môžete buď smerovať traffic nezávisle, alebo použiť funkcie spájania kanálov z Linuxového jadra 2.4, aby ste spojili všetky Vaše spojenia do jednej veľkej rúry. Tento operačný mód je nový, experimentálny a ponechaný ako úloha pre čitateľov (hej, ak ste niečo ako ja, nemôžete vystáť ďalšie úlohy vo svojom živote).

7.4 Repeatre

Nanešťastie, nie vždy je možná priama viditeľnosť na dlhú vzdialenosť. Niekedy môžete naraziť na prekážku, ponad (alebo cez) ktorú sa jednoducho nemôžete dostať. Alebo možno potrebujete predĺžiť spoj ďalej ako to umožňuje Vaše rádio a anténa. Možno ste práve na hranici dosahu dobrého AP, ale potrebujete poskytovať prístup pre oblasť plnú ľudí (a nie každý z nich má vysoko ziskovú anténu). Vo Vašom prípade môže pomôcť repeater.

Rádio repeater je zariadenie s dvoma kompletnými rádiami v sebe. Každý traffic zachytený prvým rádiom je zopakovaný na druhom a opačne. Ak sú použité smerové antény, slabý signál, dosahujúci jeden z vysieláčov, je následne znova odvysielaný cez druhý kanál, ako keby pochádzal z tohoto bodu. [Obrázok 7-4](#) znázorňuje použitie tejto techniky na rozšírenie dosahu, alebo obídenie prekážky.



Obrázok 7-4. Repeater robí jednoducho toto: opakuje všetko čo počuje niekomu ďalšiemu na konci spoja.

Hoci klasický rádio repeater môže fungovať dobre s 802.11b, ja nanešťastie nemám prístup k rádiovému zariadeniu schopnému vysielat 25MHz široký signál pri 2.4GHz. Ale mám druhú najlepšiu vec: dvojicu 802.11b PCMCIA kariet.

Nasledujúci odsek popisuje dve ako-repeater konfigurácie, ktoré úspešne používam.

7.4.1 Dve karty v jednom PC

Ak máte PC s dvoma PCMCIA slotmi, môžete nakonfigurovať Linux tak, aby používal obidva rozhrania a prepúšťal pakety medzi nimi. Zasuňte dve bezdrôtové karty a máte hardvér potrebný pre vytvorenie repeatera. Hoci mnoho klientských kariet výslovne znemožňuje Ethernetové premostenie, stále môžete použiť maškarádu medzi rozhraniami, aby ste spojili siete dokopy.

Jedno neobvyklé prenosné zariadenie, ktoré funguje dobre ako repeater, je Fujitsu Stylistic 1000. Je to staré 486/100 tablet PC, ktoré obsahuje monochromatickú LCD obrazovku, snímacie pero, 200MB PCMCIA hard disk, žiadnu klávesnicu, všetky obvyklé PC porty, lítiovú batériu a dva extra PCMCIA sloty. Môžete ich dostať u predajcov použitých počítačov za cca. 100 USD. (Ďakujem partii BAWUG za nájdenie týchto šikovných malých zariadení !)

Pozrite si detaily, v [kapitole 5](#), ako Linux nainštalovať a nakonfigurovať pre maškarádu. Keď už máte softvér nakonfigurovaný, jediná zostávajúca otázka je táto: ako natlačiť jednu kartu na vrchu druhej? Veľa bezdrôtových kariet má drobný výčnievajúci výklenok, aby urobili priestor pre ich internú anténu a nezapadnú do nadstavenej PCMCIA kazety.

Je niekoľko spôsobov ako sa vysporiadať s týmto problémom. Samozrejme, ak používate kartu ako je Cisco LMC35x pre spodnú kartu, táto nemá žiadny výklenok a preto nie je žiadny problém. Ak používate kartu ako je D-Link DWL-650¹³, je výklenok dosť malý na to, aby ste mohli vložiť dve karty naraz. Ak používate kartu Orinoco na spodku, Vaša jediná záchrana je otvoriť plastový kryt a vybrať dané dve strieborné držiaky interných antén. Po tomto budú karty viac, alebo menej, nepoužiteľné bez externej antény, ale môže sa to hodiť ak ste tlačení časom (alebo peniazmi) a máte kartu, ktorú ste ochotný obetovať pre spoj na dlhú vzdialenosť. Nezabudnite pripojiť externé antény ku obidvom rádiám, keď ich používate v jednom stroji, inak budú vysielacie pracovať hneď vedľa seba a spôsobovať obrovské množstvo interferencií.

Táto technika, zobrazená na [obrázku 7-5](#), je lacná, ale má značnú nevýhodu, že dané dve siete nie sú v skutočnosti premostené, ale sú spojené cez NAT box. Aj keď to môže vyhovovať Vašim zámerom, veľmi Vám to nepomôže, ak obe siete potrebujú byť spolu spojené priamo. Ak potrebujete premostenie medzi sieťami, poobzerajte sa za profesionálnejším zariadením, ako je Cisco Ethernet Bridge, alebo Orinoco AP-1000. Respektíve, môžete vyskúšať metódu popísanú v nasledujúcom odseku.



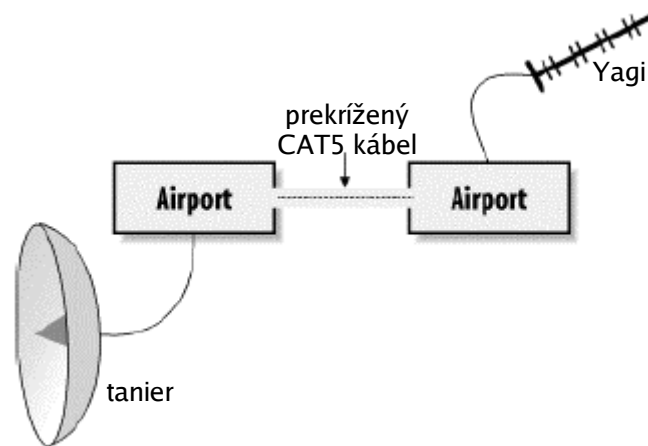
Obrázok 7-5. Dve Orinoco karty v jednom PC

¹³Na <http://kevlar.burdell.org/~will/antenna/> si pozrite jeden rýchly spôsob ako pridať externú anténu ku DWL-650.

7.4.2 Dva AP Back-to-Back (chrbtom k sebe)

Mnoho AP je schopných premostenia bezdrôtovej siete priamo na kábel. Čo sa stane ak spojíte dva AP v premostovacom móde back-to-back cez prekrížený CAT5 kábel? Prirodzene, máte premostovací repeater.

Ja som to skúšal len s dvoma Apple AirPort, znázornené na [obrázku 7-6](#), ale teoreticky, hociktoré AP schopné premostovacieho módu, by malo fungovať dobre. Pri tejto konfigurácii, každý kto je v dosahu AP A, bude mať svoj traffic zopakovaný, od slova do slova, na AP B a opačne. Keďže, Apple AirPort v skutočnosti používa rádiovú kartu Orinoco Silver, je konektor potrebný pre externú anténu už prítomný vnútri UFO. V skutočnosti, po odstránení vonkajšej škrupiny, je možné namontovať oba AirPort-y do jednej, malej, vodotesnej škatule, pričom je každý pripojený k jeho vlastnej smerovej anténe. Každý AirPort môže byť dokonca nakonfigurovaný so svojim vlastným kanálom a bezpečnostnými nastaveniami, ak je to potrebné. Výkonnosť nebude tak optimálna, ako pri priamom spoji (pretože ste zdvojnásobili možnosť kolízií), ale umožňuje to spojenie tam, kde by inak nebolo možné.



Obrázok 7-6. Dva Apple AirPort-y v premostovacom móde, spojené prekríženým káblom, môžu slúžiť ako 802.11b repeater.

7.5 Starosť o bezpečnosť

Pri používaní otvorenej bezdrôtovej siete je všetok traffic medzi Vaším laptopom a AP posielaný v zrozumiteľnej forme, každému v dosahu. Keď používate WEP, každý, kto zdieľa ten istý WEP kľúč, môže odpočúvať Váš traffic rovnako, ako keby to bola otvorená sieť. Ako môžete chrániť Vaše dáta pred zvedavými očami keď používate bezdrôt? Najlepšiu možnú ochranu poskytuje šifrovanie end-to-end (od začiatku po koniec). To je poskytované nástrojmi ako sú SSL, PPTP a SSH. Napríklad pri prezeraní stránky zabezpečenej pomocou SSL, ostane Vaša komunikácia súkromnou, zanechajúc pre všetkých, ktorí prípadne tajne odpočúvajú, dáta, ktoré vyzerajú presne ako šum spoja. Šifrovacie a identifikačné prostriedky, ktoré poskytuje 128 bitová implementácia SSL, sú všeobecne považované ako dosť dobré, pre použitie pri nedôveryhodných sieťach, ako je bezdrôt.

SSL môže byť dobrý pre web stránky (a niektorých mailových klientov), ale čo s ochranou ostatného trafficu? Tento odsek popisuje jednu metódu pre ochranu Vášho emailu použitím OpenSSH¹⁴. Pre dôkladnejšie preskúmanie možností SSH vrele doporučujem knihu *SSH: The Secure Shell*, ktorú tiež vydalo nakladateľstvo O'Reilly.

¹⁴OpenSSH je free, open source implementácia SSH protokolu. Môžete ju získať online na <http://www.openssh.com/>.

OpenSSH je vyvíjaná pre BSD, ale vďaka obrovskému úsiliu ich portovacieho tímu, je skompilovaná pod viacerými ako–Unix operačnými systémami (vrátane Linux, Solaris, HP/UX, MacOS X a veľa ďalších). Dokonca to môžete používať pod Windows, ak použijete balík Cygwin. Pozrite si <http://www.cygwin.com/> a hneď si to stiahnite, ak to ešte nemáte. Takmer to robí Windows zábavným na použitie!

Stiahnite si OpenSSH a zostavte ho. Tiež budete potrebovať kópiu knižníc OpenSSL na skompilovanie OpenSSH. OpenSSL môžete získať na <http://www.openssl.org/>. Keď už máte nainštalované OpenSSH, môžete ho použiť na tunelovanie POP trafficu z Vášho lokálneho laptopu na Váš mail server (nazývaný „mailhost“). Pre účely tohto príkladu budeme predpokladať, že máte shell-ovský účet na mail serveri, hoci každý stroj vo Vašej internej sieti, ktorý prijíma SSH spojenia, by mal postačovať.

7.5.1 Nadviazanie spojenia

Pod OpenSSH:

```
laptop# ssh -L 110:mailhost:110 -l user -N mailhost
```

(Prirodzene, nahraďte *user* Vaším užívateľským menom a *mailhost* menom Vášho mail servera, alebo IP adresou.) Uvedomte si, že pre tento príklad, musíte byť root na Vašom laptopu, kým sa pripojíte na privilegovaný port (110, POP port). Tiež by ste mali vypnúť všetkých lokálne bežiacich POP démonov (pozri do */etc/inetd.conf*), inak sa Vám postavia do cesty.

Predpokladám, že máte Váš RSA, alebo DSA kľúč nastavený, dokonca to môžete spustiť na pozadí (jednoducho pridajte *&*). Toto nastaví tunel a začne, cez neho, preposielať Váš lokálny port na vzdialený koniec. Prepínač *-N* povie SSH, aby sa neunúval spustiť aktuálny príkaz na vzdialenom konci, ale len jednoducho vykonával preposielanie.

7.5.2 Nakonfigurujte Váš mailový softvér

Teraz potrebujete povedať Vášmu mailovému softvéru, aby sa pripojil k Vášmu tunelu, miesto pripojenia sa priamo k Vášmu mail serveru. To je odlišné v každej aplikácii, ale myšlienka je vždy rovnaká: potrebujete, aby sa Váš emailový klient pripojil ku *localhost*, namiesto *mailhost*.

Tu je postup, ako to nastaviť v Netscape Communicator-e, iní klienti môžu mať rozdielne výberové menu, ale princíp je rovnaký:

- Choďte do Edit -> Preferences.
- Rozbaľte strom Mail & Newsgroups a vyberte Mail Servers.
- Vymažte Váš existujúci server prichádzajúcej pošty a pridajte nový.
- Pod General, napíšte localhost ako Server Name. Vyberte POP3 ako Server Type.
- Kliknite na OK, presvedčte sa, že Váš tunel je zriadený a stiahnite Váš mail.

Samozrejme, nemusí to končiť s POP. Tiež môžete preposielať SMTP pre odchádzajúcu poštu (port 25). Jednoducho špecifikujte viacnásobné *-L* vstupy, napr.:

```
laptop# ssh -L 110:mailhost:110 -L 25:mailhost:25 -l user -N mailhost
```

Teraz už len nastavte Váš server odchádzajúcej pošty na *localhost* a všetok Váš prichádzajúci a odchádzajúci email bude chránený pred zvedavými očami (vlastne ušami) na Vašej bezdrôtovej sieti.

7.6 Captive „Catch and Release“ Portal

(uväzňovací „chyť a prepust“ portál)

Aj keď niektorí vlastníci uzlov sú úplne šťastný pri otváraní ich sietí každému kto sa ocitne v dosahu, mnohí z nás sa zdráhajú myšlienky platiť za susedov, pri používaní našej šírky pásma. Napokon, okrem používania zdrojov za ktoré platíme, anonymný užívateľ by mohli potenciálne zneužiť ďalšie siete a zanechať stopy po ich zlomyseľnostiach späť k Vašej sieti! Ak chceme poskytovať solídny bezdrôtový prístup, potrebujeme spôsob, ako bezpečne identifikovať užívateľov, keď sa pripájajú a potom prideliť len tie zdroje, ktoré je vlastník uzla ochotný poskytnúť. Po summite v Portlande bolo zrejmé, že jeden kľúčový komponent, ktorý sa vytratil z myšlienky komunitnej siete, je voľne dostupná implementácia *captive portal-u* (uväzňovací portál).

Myšlienka, ktorá je za captive portálom, je úplne zrejmá. Namiesto spoliehania sa na vstavané bezpečnostné prvky 802.11b na riadenie toho, kto sa môže pripojiť ku AP, nakonfigurujeme AP bez WEP a ako otvorenú sieť. Dané AP je tiež v premostovacom móde a pripojené cez prekrížený kábel ku Ethernetovej karte na Linuxovom router-i. Potom je už na router-i, vydávať DHCP licencie, regulovať šírku pásma a povoľovať prístup ku ďalším sieťam. Keď sa užívateľ pokúsi prezerať si nejakú web stránku, je presmerovaný na stránku, ktorá predkladá informácie o danom užívateľovi s výzvou na prihlásenie a informáciami o uzle, ku ktorému sa pripojil. Ak má bezdrôtová brána spôsob, ako kontaktovať centrálnu autoritu, kvôli určeniu identity pripojeného bezdrôtového užívateľa, potom môže primerane zmierniť pravidlá firewallu, tak že poskytne privilégia patriace danému užívateľovi (napr.: väčšiu šírku pásma, alebo prístup ku iným strojom a portom).

Projekt *NoCatAuth* implementuje autentifikačný systém tretej strany. Napísaný je v Perl-e a C-čku, stará sa o prihlásenie užívateľa pomocou prihlasovacej výzvy, kontaktuje MySQL databázu, aby vyhľadal užívateľove dokumenty, bezpečne oboznámi bezdrôtovú bránu o užívateľovom statuse a autorizuje ďalšie prístupy. Na strane brány riadi softvér lokálne spojenia, nastavuje reguláciu šírky pásma a pravidlá firewallu a odpája (times out) staré prihlásenia, po uplynutí užívateľom špecifikovaného časového limitu. Softvér je vydaný pod GPL.

Navrhli sme systém tak, že dôvera je skutočne zachovaná, brány a koncoví užívatelia potrebujú dôverovať len autentifikačnému systému, ktorý je chránený registrovaným SSL certifikátom. Heslá nie sú nikdy dané bezdrôtovej bráne (takto sú chránení užívatelia pred „zlými chlapcami“ vlastniami brány) a pravidlá brány sú modifikované len pomocou kryptograficky podpísanej správy od autentifikačného systému (chrániac bránu pred užívateľmi, alebo upstream stránkami, pokúšajúcimi sa napodobniť autentifikačný systém).

My rozlišujeme tri možné triedy bezdrôtových užívateľov:

- verejná trieda
- co-op trieda
- trieda vlastníka

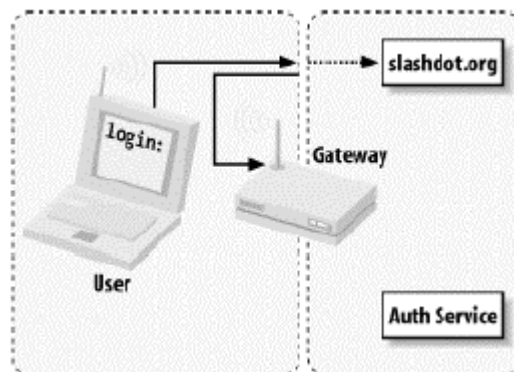
Užívateľ *verejnej triedy*, by mal byť niekto, kto nevie nič o miestnej bezdrôtovej skupine a len jednoducho hľadá prístup na Internet. Tejto triede je pridelená veľmi malá šírka pásma a užívateľ má obmedzené, ku ktorým službám môže pristupovať, použitím pravidiel firewallu. Verejnej triede užívateľov je daná možnosť dozvedieť sa viac o tom, kto poskytuje bezdrôtovú službu a ako sa môžu skontaktovať s miestnou skupinou (a napokon získať väčší prístup). Nemajú osobné prihlásenie, ale predsa len sa musia

autentifikovať manuálnym preskočením prihlasovacieho procesu (odtiaľ výraz *catch and release* – chyť a prepusti).

Co-op trieda pozostáva z užívateľov s predpripravenými prihlasovacími informáciami. Pravidlá pre členov by mali byť stanovené miestnou komunitnou skupinou a sú nakonfigurované v centrálnej databáze autentifikačného systému. Tejto triede je obvykle pridelená omnoho väčšia šírka pásma a prístup k portom, užívatelia môžu byť braný na zodpovednosť za ich vlastnú činnosť.

Trieda vlastníka je takmer rovnaká ako co-op trieda, ale je rezervovaná pre vlastníka daného uzla a hocikoho ďalšieho, komu on chce prideliť prístup. Trieda vlastníka predbehne traffic všetkých ostatných tried a má voľné použitie všetkých sieťových zdrojov.

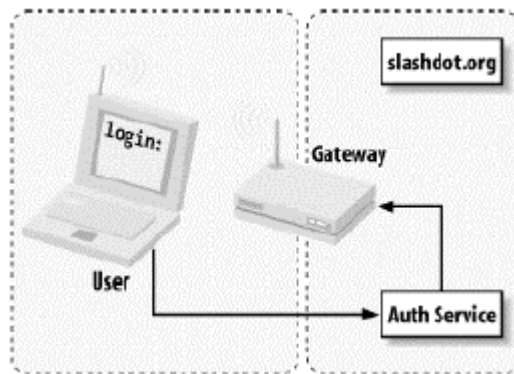
Typický pripájací proces začína, keď sa potulujúci užívateľ spojí s AP a má okamžite pridelenú DHCP licenciu, ako je znázornené na [obrázku 7-7](#). Všetok prístup, okrem kontaktovania autentifikačného systému, je štandardne zamietnutý. Keď sa užívateľ pokúsi prezerať web, je neodkladne presmerovaný na službu brány, ktorá ho následne presmeruje na SSL prihlasovaciu stránku autentifikačného systému (po pridaní náhodného rámca a nejakých ďalších informácií ku URL linke).



Obrázok 7-7. Užívateľ má okamžite vydanú licenciu a jeho prvé web pripojenie je presmerované na službu bezdrôtovej brány.

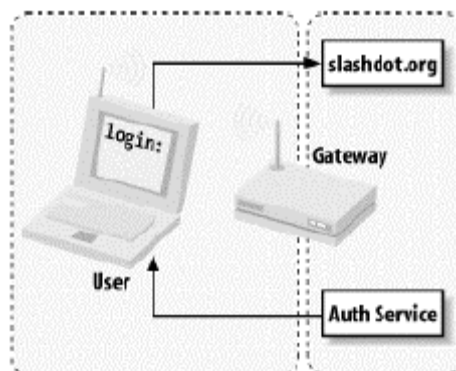
Daný užívateľ má potom tri možnosti: prihlásiť sa s predpripravenými prihlasovacími informáciami, kliknúť na odkaz, aby získal viac informácií o členstve, alebo kliknúť na tlačítko *Skip Login* (preskoč prihlásenie).

Keď sa užívateľ, buď korektne prihlási, alebo preskočí prihlásenie, autentifikačný systém následne vytvorí výslednú správu, podpíše ju pomocou PGP a zašle späť bezdrôtovej bráne (viď [obrázok 7-8](#)). Brána má kópiu verejného kľúča autentifikačnej služby a dokáže overiť pôvod správy. Časť dát vložených do odpovede je daný náhodný rámec, ktorý brána pôvodne vydala klientovi, čo má za dôsledok, že je veľmi ťažké oklamať bránu pomocou „replay attack“ (opakovaný útok). Digitálny podpis bráni možnosti, aby sa iný stroj tváril ako autentifikačná služba a posielal falošné správy bezdrôtovej bráne.



Obrázok 7-8. Po prihlásení sa autentifikačný systém spojí späť s bezdrôtovou bránou a oboznámi ju s výsledkom, brána sa potom dokáže rozhodnúť, či povolí, alebo nie, ďalší prístup.

Teraz, ak všetko prebehlo pre užívateľa dobre, bezdrôtová brána modifikuje svoje pravidlá firewallu, aby povolila ďalší prístup a presmeruje užívateľa naspäť na tú stránku, ktorú sa pôvodne pokúšal prezerať (tak, ako je to znázornené na [obrázku 7-9](#)).



Obrázok 7-9. Daný užívateľ teraz môže pokračovať vo svojej šťastnej ceste.

Aby sa udržalo spojenie otvorené, je na strane klienta otvorené malé okno (pomocou JavaScriptu), ktoré občerstvuje prihlasovaciu stránku každých pár minút. Keď sa užívateľ dostane mimo oblasti, alebo zavrie svoj prehliadač, je spojenie resetované a požaduje ďalšie manuálne prihlásenie.

Požiadavky na strane brány sú minimálne (systém bol navrhnutý tak, aby bežal pod Linuxom 2.4.5 na 486 so 16MB RAM). Autentifikačný systém je navrhnutý tak, aby bol spravovaný komunitnou skupinou, ktorá udržiava svoju užívateľskú databázu, akýmkoľvek vhodným spôsobom. Napríklad, prevádzkovanie uzla je jeden z očividných spôsobov ako sa stať členom co-op. Ale to nie je vždy najlepší spôsob, ako vynaložiť so zdrojmi; ľudia, ktorí poskytnú hardvér, programovacie vedomosti, šírku pásma, alebo dokonca priestor na stretávanie a občerstvenie, by mali byť určite prijatí za členov. Technické aspekty portálu sa riešia a je na každom, aby pracoval na sociálnych detailoch.

NoCatAuth systém je stále v aktívnom vývoji. Vždy môžete získať najnovšiu verziu z <http://nocat.net/>.

7.7 Na záver

802.11b hardvér sa zdá byť limitovaný len predstavivosťou tých, ktorí naň môžu položiť svoje ruky, a s postupom času klesajúcimi cenami, sa bude počet ľudí, ktorí sa v ňom vrtajú, len zvyšovať. Ak Vás zaujalo rozširovanie zariadení, prihláste sa k niektorej skvelej bezdrôtovej diskusnej skupine, kúpte si nejaké zariadenie a začnite.

Kapitola 8. Radio Free Planet

Uplynulý rok ukázal explóziu záujmu o výstavbu bezdrôtových verejných sietí. Všadeprítomnosť cenovo prístupných 802.11b zariadení podnietila enormný záujem o rozšírenie Net-u a poskytovanie otvoreného (alebo za veľmi nízku cenu) prístupu naň. Táto myšlienka sa zdá byť takmer nevyhnutná: ak väčší bezdrôtoví poskytovatelia účtujú tridsať dolárov a viac *za mesiac*, za nízku rýchlosť, neistý bezdrôtový sieťový prístup a nástroje sú dostupné na to, aby Vám poskytovali vysoko rýchlostný prístup, za veľmi nízku cenu, prečo sa nespojiť a nezrealizovať to? Ľudia po celom svete, ktorí majú spoločný sen o všadeprítomnej neobmedzenej voľnej šírke pásma, budujú ich vlastné všadeprítomné vysoko rýchlostné siete. Ľudia budujú potrebnú infraštruktúru, aby poskytli sieťový prístup tisícom paralelných užívateľov za, pre nich, veľmi nízku cenu, spoluprácou a používaním otvorených štandardov. Všade ľudia dokazujú, že je to omnoho praktickejšie ako služba spolupracujúcej komunity, než ako komerčný podnik s prvotným zámerom finančného zisku.

Keď som začal pracovať na tejto knihe začiatkom 2001, existovalo snáď 10 dobre známych bezdrôtových skupín. Keď toto píšem obsahuje zoznam bezdrôtových komunít Personal Telco (<http://www.personaltelco.net/index.cgi/WirelessCommunities>) viac ako 50 nezávislých komunitných bezdrôtových skupín. Tu je zopár najväčších a najunikátnejších projektov, na ktoré som natrafil. Toto ich predstavenie, by Vám malo dať predstavu o tom, o čo vlastne ide (možno dokonca vo Vašom susedstve).

8.1 Bezdrôtový Seattle

Bezdrôtový Seattle (<http://www.seattlewireless.net/>) je jeden z najambicióznejších projektov zo všetkých komunitných skupín: má v úmysle vybudovať plne smerovanú metropolitnú sieť, nezávislú na žiadnom poskytovateľovi komerčných služieb. Doteraz, nastavili ich vlastné top-level DNS domény, prideliť súkromné IP adresy, nastavili chrbticové uzly a riadia rozloženie siete tak, že každý bezdrôtový uzol, bude schopný dosiahnuť ktorýkoľvek iný, dokonca bez potreby prenášať pakety cez komerčnú sieť. Keďže každý chrbticový uzol je schopný poskytovať služby Internetovej brány, bezdrôtoví klienti tiež môžu pristupovať na Internet, bez ohľadu na to, kde sa fyzicky v meste nachádzajú.

Keďže celá bezdrôtová sieť sa vôbec nespolieha na kábel, drží to prevádzkové náklady siete fixné a tiež môže poskytnúť hodnotné komunikačné služby v prípade väčších katastrof (Seattle nie je práve známy svojou stabilitou, v mnohých smeroch). Seattle má niektoré unikátne geografické výhody, ktoré môžu pomôcť tejto koncepcii: relatívne málo stromov, veľa vysokých budov, mierne kopce a vysokú koncentráciu technicky zdatných ľudí. Som si istý, že káva neškodí.

Ich web stránka je ohromne bohatá na informácie, od teórie smerovania sietí, po konštrukciu antén. Stránka Seattle Wireless bola spustená v septembri 2000. Odvtedy boli spomenutý vo viac ako 35 publikáciách, siahajúcich od magazínu *Wired*, po

Le Monde, veľké noviny vo Francúzsku. Majú tiež obrovskú diskusnú skupinu a poriadajú pravidelné stretnutia. Svoju činnosť vykonávajú v Great Northwest.

8.2 BAWUG

Bay Area Wireless User's Group (<http://www.bawug.org/>) je jedna z niekoľkých bezdrôtových skupín v oblasti San Franciského zálivu. Vyvinula sa z Playa Net, free 802.11b siete Burning Man (detaily viď <http://www.playanet.org> a <http://www.burningman.com/>). Keďže obrovské percento účastníkov Burning Man je zo San Franciska, bolo len prirodzené, že 10-denný užívatelia siete, by chceli niečo na zvyšných 355.

Aj keď sa predovšetkým zameriavajú na vzdelávanie, skupina BAWUG je obrovským príspevkom pre svetové bezdrôtové komunity ich web stránkou a pravidelnými stretnutiami. Členovia si pomáhajú skupinovými nákupmi zariadení, odviekli kus práce pri hľadaní cesty labyrintom FCC Part 15, a celkom dobre si počínajú, aby splnili ich kolektívny cieľ:

BAWUG poskytuje pomoc pri vývoji infraštruktúry poskytnutím: diskusnej skupiny, servisu, vzdelávania, atď. vrátane každomesačných stretnutí. Náš aktuálny cieľ je vydávať dokumenty na pomoc bezdrôtovým komunitám, druhoradá je vybudovať komunitnú sieť.

Oni tiež priniesli úplne prvú online porovnávaciu databázu bezdrôtového hardvéru. Tento nástroj je zadarmo (a neoceniteľný) pre každého, kto používa komerčné AP. Oni zbierajú aktuálne štatistiky výkonnosti a údaje (vrátane dosahu, priepustnosti, ceny a jednoduchosti používania) o každom kuse hardvéru, ktorý sa im mohol dostať do rúk. Databáza je udržiavaná užívateľmi. Detaily si určite pozrite na ich stránke. Ak ste dokonca v oblasti SF zálivu, vrelo Vám doporučujem zúčastniť sa stretnutia. Vždy pritiahnu viac ako 50 ľudí a pozývajú skupinu zaujímavých rečníkov zameraných na bezdrôtový priemysel, cez Internet, po RF inžinierov. Naša skupina sa vždy zúčastnila, bolo dobre umiestnené, dve hodiny jazdy zo Sebastopol-u.

8.3 Personal Telco

Jedna z pár skupín v Portlande, v oblasti Oregon, Personal Telco Project (<http://www.personaltelco.net/>) tiež pomáha budovať komunitu v oblasti Pacific Northwest. Tak ako mnohí z nás, sú zakladatelia nespokojný s premrštenými poplatkami za sieťový prístup a otrasnou neochotou ľudí poskytujúcich komerčnú podporu. Špecifikujú detailné hardvérové riešenie pre všetkých ich členov, robia obsluhu uzlov tak jednoduchú, ako sa to len dá a rozširujú ich sieť veľmi rýchlo.

Prevádzkujú diskusnú skupinu a riadny IRC kanál (#*personaltelco* na irc.openprojects.net) a usporiadali vôbec prvé svetové stretnutie Wireless Summit (viď diskusia o summite v kapitole 9 a online správa na <http://www.personaltelco.net/index.cgi/SummitJune2001>). Ich diskusná skupina je výborný zdroj informácií a skvelá debata.

8.4 NYC Wireless

Obrovské úsilie priniesť voľné uzly s Internetovým online prístupom badať v New York City. Aby som citoval ich web stránku:

Sieť je slobodná (free), rovnako ako je slobodná reč a slobodné pivo.
Každý AP je prevádzkovaný nezávisle, dobrovoľníkmi, s ich vlastnými zariadeniami.

Skupina NYC Wireless vydala niekoľko dovedy neriešených záležitostí, vrátane Power over Ethernet HOWTO. Tiež sa zaoberajú možnosťou registrácie ako nezisková organizácia a ponúkať služby distribúcie zdrojov pre ich členov a iným komunitným skupinám. Ich úsilie nezostalo nepovšimnuté populárnou tlačou, dokonca boli spomenutý v CNN, ohľadom ich práce na poskytovaní verejného sieťového prístupu.

Môžete ich nájsť online na <http://www.nycwireless.net/>, kde prevádzkujú FAQ, diskusnú skupinu, mapu uzlov a ďalšie zdroje.

8.5 GBPPR

Skupina Green Bay Professional Packet Radio (z Green Bay, Wisconsin) je zriedkavá skupina, prechádzajúca na bezdrôtovú stavbu sietí so solídnymi znalosťami z rádio technológií. Aj keď nie sú obzvlášť zameraný na 802.11b, majú obrovské bohatstvo informácií o konštrukcii rádii. Exotické technológie, ako je spoj bod-bod laserový lúčom, konštrukcia fraktálovej antény a doma vyrobený spektrálny analyzátor sú len niektoré zo zábavných vecí, ktoré nájdete na GBPPR. Ich hlavná stránka je online na <http://www.qsl.net/n9zia/index.html>.

Tiež prevádzkujú skupinu šialene užitočných interaktívnych výpočtových nástrojov. Ak potrebujete určiť fresnelovú zónu, natočenie a zdvih antény, alebo množstvo zisku potrebného na prekonanie určitej vzdialenosti, musíte si pozrieť ich free, interaktívny softvér na návrh rádii. Môžete to nájsť online na <http://www.qsl.net/n9zia/wireless/page09.html>. Konkrétne pre mňa bol ich nástroj Wireless Network Link Analysis neoceniteľný pre odhad straty cestou a stanovenie rozpočtu spoja (niekoľko príkladov, ako to vypočítať pre svoje potreby, si pozrite v kapitole 7 a potom použite ich vynikajúci nástroj na hru „čo ak“).

8.6 GAWD

Skupina Shmoo vytvára GAWD, Global Access Wireless Database. Hoci nie sú skutočná bezdrôtová komunitná skupina, služba, ktorú poskytujú, je veľmi zaujímavá. Ich nástroj umožňuje bezdrôtovým poskytovateľom a skupinám vypísať fyzické umiestnenie a schopnosti ich AP. Údaje sa potom dajú vyhľadávať podľa poskytovateľa, umiestnenia, alebo dokonca podľa zemepisnej šírky a dĺžky. Keď toto píšem majú 211 AP v online zozname. Môžete si pozrieť GAWD (a vypísať Váš vlastný uzol) na <http://www.shmoo.com/gawd/>.

8.7 Guerrilla.net

Nespokojný s tým, že sú spájaný s konkrétnou bezdrôtovou technológiou, alebo dokonca s poskytovaním Internetového prístupu, usiluje sa skupina Guerrilla.net z Bostonu udržať nažive tok informácií:

Keďže je vyvíjaný nátlak na Internet zo strany nebezpečných indivíduí vo vláde USA, je potrebná *alternatívna* sieť, aby zaistila, že slobodný tok informácií nie je zatarasovaný, odchyťovaný, analyzovaný, modifikovaný, alebo zaznamenávaný. To je hlavný zámer guerrilla.net... Slobodný tok súkromných informácií je POŽIADAVKA slobodnej spoločnosti.

Prevádzkujú impozantnú technickú knižnicu, vrátane informácií o stavbe antén, nastavovaní bod-bod a verejne prístupných spojov a bezdrôtových technológií, od UHF po 10GHz. Obsahuje zoznam niekoľkých rádiových módov a dokonca plány na 6dbi všesmerovú anténu. Dajú sa nájsť online na <http://www.querrilla.net/>.

8.8 Universal Wireless

Fenomén komunitných sietí s verejným prístupom určite nie je obmedzený na Severnú Ameriku. Takmer polovica bezdrôtových projektov uvedená na zozname komunity Personal Telco sa nachádza mimo USA. Projekty sa začali v Anglicku, Nemecku, Švédsku, Francúzsku, Fínsku, Holandsku, Austrálii a v mnohých ďalších krajinách. Ja osobne som bol kontaktovaný ľuďmi zaujímavými sa o nekáblové mestá v Tibete, Kanade a Mexiku. Podľa všetkého sa zdá, že čas komunitných bezdrôtových sietí konečne prišiel.

Kapitola 9. Radio Free Sebastopol

Môj prvý kontakt s 802.11b sieťami v lete 2000 bol pre mňa už vtedy niečím úplne jasným: bolo zrejmé, že bezdrôtová konektivita sa stane úžasne dôležitou technológiou. V nasledujúcom roku sa vyrojili tucty miestnych komunitných bezdrôtových skupín (a dokonca aj zopár komerčných firiem), budujúcich použiteľné siete vzduchom s využitím 802.11b zariadení. Toto je príbeh o tom, ako sa zrodila myšlienka urobiť našu podnikovú sieť flexibilnejšou a ako sa stala časťou celosvetového trendu, poskytovať všadeprítomný bezdrôtový sieťový prístup.

9.1 OSCON 2000

Moje prvé oboznámenie sa s bezdrôtovými sieťami bolo v Monterey, California na OSCON (Open Source Conference) 2000. O'Reilly zriadil voľný verejný prístup pre účastníkov konferencie. Ohromná flexibilita, byť schopný sa pripojiť ku sieti zovšadiaľ, viedla ku všetkým druhom záujmu a neobvyklej interakcie. Napríklad, ľudia zúčastnení veľkej diskusie, mohli konverzovať v reálnom čase cez IRC a diskutovať o téme (a dokonca kritizovať rečníka) bez zvýšenia hlasu. Mohli používať Net ako zdroj pri kladení otázok rečníkovi, vysvetliť veľmi zaujímavé body pomocou príkladov v reálnom čase. Všadeprítomný bezdrôt s instant messaging klientom vytvoril efektívny, voľný, dvojcestný, dorozumievací systém. (Namiesto pokúšania sa použiť preťažený PCS telefónny systém bolo možné poslať rýchlu správu „Kde sa stretneme na obed?“ a dostať okamžite späť odpoveď.) Účastníci konferencie sa viac nemuseli vraciť do svojich hotelových izieb kvôli dial-up prístupu, alebo byť vyhostení do miestnosti s terminálmi, mimo diania, len aby si skontrolovali email, alebo pozreli web stránku. Samozrejme, to predpokladalo, že dotyčný má poruke 802.11b kartu a laptop. Ja osobne, som vybojoval kartu od chlapíka, ktorý mal náhradnú. Uvedomil som si, že si jednoducho musím pribaliť svoju vlastnú.

Po návrate z OSCON malo O'Reilly veľký záujem o sprevádzkovanie bezdrôtovej siete vo svojich kanceláriách. Ak niečo tak flexibilné, môže byť vybudované tak veľmi lacno, prečo by sme to nepoužívali doma? Ak to dokážu využiť účastníci konferencie na omnoho efektívnejšie získavanie informácií, čo by to mohlo urobiť pre naše firemné schôdze a prezentácie? A tak, dokonca bez väčších vedomostí, som začal dlhú, kľukatú cestu bezdrôtového sieťovania.

9.1.1 Areál

Po nastavení pár AP, aby pokryli náš areál a katastrofálnom kurze WEP, MAC filtrovania a uzavretých sietí, bola naša 802.11b sieť hotová. S relatívne malým úsilím a cenou (cca. 3000 USD a celkovo zopár hodín práce), máme teraz celistvé pokrytie vo všetkých troch našich budovách, kompletne aj s roaming-om medzi AP. Hlavné ústredie O'Reilly v Sebastopol-e pozostáva z troch budov, zaberajúcich plochu cca. 450 krát 150 stôp. Použitím jedného Lucent AP-1000 v každej budove a malej 5db všesmerovky pri každom AP, som bol schopný pokryť takmer všetky kancelárie a konferenčné miestnosti.

Ešte na začiatku, jeden z našich užívateľov upozornil, že sa nemôže dostať online, dokonca napriek tomu, že mal veľmi silný signál. Po skontrolovaní jeho sieťových nastavení som si uvedomil, že nemá nastavený náš ESSID a tak sa môže pripájať na hocikakú dostupnú sieť. Tak sa zdalo, že sieť so silnejším signálom prichádza z firmy vo vedľajších dverách! Naštartoval som nástroj Site Map od Lucentu a naozaj, hneď vo vedľajších dverách bola už existujúca 802.11b sieť. Po rýchlej konverzácii s ich sysadminom sme sa dohodli na číslovacej schéme kanálov, tak aby sa minimalizovala interferencia medzi danými dvoma sieťami. (To je presne dôvod, prečo je predbežná prehliadka lokality tak dôležitá: dokonca aj keď nemusíte vidieť antény, môže už vo Vašej oblasti existovať sieť! Jednoducho nepredpokladajte, že keď je bezdrôt nový pre Vás, je nový aj pre Vašu časť mesta.)

Teraz sú naše kancelárie nasýtené prístupom, s viac ako 50 šťastne odviazanými užívateľmi, čo by sme s tým mohli robiť ďalej? Prirodzene, viac než len zopár očí sa otočilo ku hotelu a kaviarni na druhej strane ulice. Ak niekto môže dostať signál z hotela, potom dochádzajúci zamestnanci, ktorí sú tam ubytovaní, môžu byť zdarma online pri 11Mbps (ako protiklad platenia za pramienok dial-up prístupu). A samozrejme, byť schopný pracovať priamo z kaviarne, to musí *niečo* urobiť s produktivitou. S predstavou kávy a šírky pásma tancujúcich v mojej hlave som sa začal zaoberať pridávaním externých antén, aby som rozšíril náš dosah.

9.1.2 Káva, káva, káva

Približne za týždeň som mal všesmerovú anténu inštalovanú na streche, dole spustených 25 stôp LMR-200 ku nášmu AP. Prečo som použil 25 stôp kábla, ktorý stratí takmer 17db signálu každých sto stôp? A prečo som použil všesmerovku, keď malá sektorová anténa by mohla mať väčší zmysel? Pretože pred rokom, bez akýchkoľvek predchádzajúcich vedomostí o rádiách, som pracoval s tým, čo mi náš predajca ponúkol: 25 stôp takzvaného „nízko stratového“ kábla k mikrovlnným anténam a drahý všesmerový cencúľ. (Vlastne, ak Lucent vyrobil dané zariadenie, potom *musí* byť kompatibilné s AP Lucent, správne?)

Našťastie pre mňa, napriek vysokej strate spoja, všesmerovka si urobila svoju robotu. To poobedie som prešiel cez ulicu, objednal si ľadovú kávu a pohotovo napísal potvrdzujúci email. Ako som stlačil *Control-X Y*, bol som nútený sa zamyslieť nad nevyhnutnou otázkou, „čo ďalej?“. Ak bolo možné dostať dobrý signál o 1500 stôp od AP, nakoľko realizovateľné by bolo poskytnúť bezdrôtový prístup našim miestnym zamestnancom? Napokon, veľa našich ľudí býva v oblasti a používali dial-up na prístup k našej sieti z domu. Bolo by možné poskytnúť rýchle bezdrôtové pripojenie každému, kto je v dosahu? Ako ďaleko môže byť táto technológia nafahovaná?

9.1.3 Online z domu, bez špeciálnych podmienok

Pred krátkym časom som sa presťahoval do Sebastopol-u zo San Franciska. Zhodou okolností, dom, do ktorého sme sa nasťahovali, mal priamu viditeľnosť na anténu, ktorú som inštaloval na streche, vzdialenú viac ako pol míle. To poskytlo vynikajúci nástroj na experimentovanie, teraz som mal stabilný signál na vzdialenosť s priamou viditeľnosťou (LOS) a môžem naň zacielať akýkoľvek typ zariadenia chcem, aby som videl, ako dobre bude slúžiť. Zistil som, že vysoko ziskový tanier, nasmerovaný priamo na všesmerovku dokáže dosiahnuť veľmi dobrý signál, dokonca aj cez steny a sklo. Bol som taký vzrušený kvalitou signálu, že som priviazal tanier na stoličku s kolieskami a tlačil ju po dome, zatiaľ čo som po celý čas pozeral video na celú obrazovku na mojom laptopu. Áno, silný záujem o bezdrôt sa teraz rozvinul do úplnej psychotickej posadnutosti, po rozume mi behali prípadné možnosti komunikácie na dlhú vzdialenosť, za nízku cenu, pri vysokej rýchlosti.

Konečne som upevnil tanier na pôjde, nastavil provizórne AP a zistil, že môžem mať stabilné 11Mbps pripojenie zo vzdialenosti šesť desiatín míle, s tanierom „skrytým“ pod mojou strechou, ktorý nebude obťažovať mojich susedov. Používal som toto spojenie niekoľko mesiacov za každého počasia (a bol som za to veľmi vďačný: v mojej oblasti, v tom čase, nebola možnosť DSL, ani káblového modemu).

Teraz, keď som urobil skúšku správnosti a mal zoznam komponentov, som sa obrátil na ostatných z firmy, ktorí bývajú v oblasti, aby sa pokúsili nastaviť druhý uzol. Vtedy som narazil na asi najväčšiu prírodnú prekážku pre dlhé mikrovlnné spoje: *stromy*. Keď k tomu prišlo, bol som skutočne šťastný z mojej vlastnej situácie. Nájdenie viacerých trás, bez prekážok, ku jednému bodu je v Sebastopol-e vysoko nepravdepodobné. Okrem bezprostrednej dolnej časti mesta, stredné až husté listie je prakticky všade. Po obhliadke niekoľkých možných polôh uzla (a vyskúšaní spojenia s O'Reilly napriek stromom) bolo jasné, že jedno AP v nízkej výške nebude postačujúce na odkáblovanie našich zamestnancov zo Sebastopol-u. Medzi O'Reilly a zvyškom sveta je jednoducho príliš veľa stromov.

Bez konkrétneho plánu ďalšej činnosti, musel som odložiť projekt rozšírenia bezdrôtu na chvíľu bokom, aby som mohol viac bádať. Vtedy bol skutočne nedostatok dostupných informácií online, keďže komunitné skupiny ešte len začínali vznikať po celom svete. Rozhodol som sa, že ak sa chcem niekam dostať s praktickou stavbou sietí, potrebujem hovoriť s nejakými expertmi.

9.1.4 Bezdrôtový Seattle

Minulý marec som si urobil výlet do Seattlu. Môj brat sa do tej oblasti presťahoval a tak som využil príležitosť cestovať s ním na sever, aby som si osobne pozrel sieť Seattle Wireless. Musím priznať, že som nebol úplne pripravený (psychicky) na to, čo tam nájdem, keď sa tam dostanem. Tam bola skupina *veľmi* ostrých sysadminov, programátorov a sieťových figliarov, ktorí budovali redundantnú, plne smerovanú, verejnú sieť, nezávislú od Internetu. Oni na tomto projekte pracovali *výhradne vo voľnom čase*, bez nároku na inú odmenu, ako je potešenie z práce na projekte, ktorý jednoducho potrebuje byť zrealizovaný. Oni, nie len jednoducho zavesili pár AP a spoliehali sa na šťastie, ale mali naplánovanú úplnú topológiu siete, vybrané hardvérové riešenie a uzly vo výstavbe na pripojenie miest vzdialených míle.

Strávil som jeden deň výstavbou antén a rozmýšľaním o možnostiach 802.11b s partiou SWN. Na konci dňa sme sa rozhodli spolu zostrojiť Yagi, vyrobenú z podložiek, nejakej trubky, skrutky a plechovky, ktorá preniesie 11Mbps signál na míľu. Topológia

Seattlu je taká, že ich sieťové plány budú zrejme fungovať: vysoké budovy, mierne kopce a obmedzené pokrytie stromami, robia väčšinu mesta dostupným (za predpokladu, že sa niekto dokáže dostať na vrch kopca). Do Sebastopol-u som sa vrátil s niekoľkými dôležitými poznatkami:

- Tam bol obrovský záujem o vysoko rýchlostnú bezdrôtovú sieť, dokonca aj medzi ľuďmi, ktorí už mali vysoko rýchlostný káblový prístup. Všadeprítomný bezdrôt sa zdal byť takmer tak veľmi žiadaný, ako DSL, alebo káblový modem.
- Zdanlivo neriešiteľná obtiažnosť nájsť LOS medzi bodmi, nemôže byť skutočne vyriešená jednou osobou, alebo skupinou. Ale väčšia, spolupracujúca komunita s rovnakým cieľom, dokáže priniesť množstvo zdrojov na vyriešenie každého problému.
- Bezdrôtová sieť nie je tak jednoduchá, ako nahradenie kusu CAT5 rádiom. Rádio má veľa podivných vlastností, ktoré sú úplne neznáme aj pre ľudí, ktorí roky študovali počítače a siete.
- Obrátene, mnoho rádio expertov sa stratilo, keď sa zaoberali podrobnosťami Internetového sieťovania (len donedávna 9600 baudové prenosné rádiové pripojenie ku počítaču bežiacemu pod DOS TCP/IP bolo považované za high tech v mnohých kruhoch). Ak mienime dotlačiť 802.11b za pôvodne zamýšľané hranice, hladina vedomostí, ktorá oddeľuje jadro sieťových džokejov od jadra rádiových geek-ov sa musí prelínať.

Paradoxne, začalo to vyzeráť, akoby bolo ľahšie odstrihnúť celú oblasť Sebastopol-u od káblu, pomocou otvoreného sieťového prístupu, namiesto pokúšania sa pripojiť pár užívateľov ku súkromnej sieti. Ale aby sa to zrealizovalo, určite som nemohol urobiť všetku prácu sám. Potreboval som zistiť, či je aj v mojej oblasti tak veľa záujmu, ako sa zdalo byť vo zvyšku krajiny.

9.1.5 NoCat (bez mačky)

Bolo nám jasné, že potrebujeme lokálny priestor pre informácie o formujúcej sa spolupracujúcej komunitnej sieti. V priebehu pár dní, niekoľko kamarátov a ja, sme dali dokopy jednoduchú web stránku a diskusnú skupinu. Ale, ako ju nazvať?

Kým som sedel na gauči v obývačke, prihlasujúc sa, aby som skontroloval niečo v práci, moja náhodná správa pri prihlásení mi odrazu pripadala obzvlášť zábavná, tak som to nahlas prečítal môjmu kamarátovi s menom Cat (mačka):

Viete, drôtový telegraf je druh veľmi, veľmi dlhej mačky. Potiahnete jej chvost v New Yorku a jej hlava zamŕnauká v Los Angeles. Rozumiete tomu? A rádio funguje presne tak isto: vy tu odošlete signál, oni ho tam prijmu. Jediný rozdiel je v tom, že je to *bez mačky*. - Albert Einstein

Cat okamžite odpovedal, „Takto by si mal nazvať tú vec: No Cat. (bez mačky)“. Okamžite som skontroloval *whois* a uvidel, že *nocat.net* je voľný. Tak sa to prijalo.

NoCat sa stal hlavným priestorom pre niekoľko bezdrôtových projektov, na ktorých sme Schuyler Erle (Perl programátor a bezdrôtový sympatizátor z O'Reilly), ja a ďalší pracovali. Dali sme dokopy WRP, wireless router-on-a-floppy (bezdrôtový router na diskete), na rýchle a bezbolestné nastavovanie bezdrôtovej brány. Tiež sme začali pracovať na projekte NoCatAuth, metóde na autentifikáciu užívateľov spolupracujúcej siete, bez použitia akejkoľvek vstavanej (a obmedzenej) metódy dostupnej v špecifikácii 802.11b. Tiež sme vytvorili diskusnú skupinu pre miestnych, zaujímajúcich sa

o bezdrôt. Teraz už máme web a dostupné nejaké informácie, potrebujeme spôsob ako sa spojiť s ľuďmi do miestnej komunity.

9.1.6 Článok

Našťastie sme nemuseli dlho čakať, kým si nás komunita všimla. Hneď, ako som sa vrátil zo Seattlu, miestne noviny *Press Democrat* (viď archív na <http://www.pressdemo.com/>, „Downtown Sebastopol Going Wireless“, publikované 2.4.2001) vydali článok o nejakých bezdrôtových chuligánstvach, ktorých som bol schopný. Nemal som v tom čase žiadnu predstavu, ako hodnotný môže byť tento druh propagácie, pre myšlienku komunitnej LAN. V priebehu týždňa som dostal zopár emailov a niekoľko telefonátov od miestnych, ktorí sa zaujímali o bezdrôtové siete. Niektorí ponúkli odbornú pomoc a zariadenie, zatiaľ čo iní boli len zvedaví na naše plány a na to, ako by sa mohli oboznámiť s 802.11b.

Po vyjdení článku naša diskusná skupina narástla na 25 ľudí. Dohodli sme sa zvoliť spoločné stretnutie, aby sme sa zorganizovali a vyjasnili čo od toho očakávame. Veľmi príjemne ma prekvapilo, keď sa na prvom stretnutí ukázalo 16 zaujímavých ľudí. Mnohí hľadali vysoko rýchlostný prístup, kým ostatní boli len jednoducho zvedaví. Zopár bolo obeťou Northpoint-u, boli násilne odpojený od ich DSL, keď sa táto spoločnosť dostala do problémov a hľadali akúkoľvek alternatívu (očividne neboli cieľovou skupinou „hlavného“ trhu a najradšej by nejakú dobu vysoko rýchlostný prístup nevideli).

Keď diskusia dobre pokračovala tretiu hodinu, bolo jasné, že sa z toho stane pravidelná udalosť. Títo ľudia sa náruživito zaujímali o príspevok k slobodnej miestnej sieti a mali úžasné množstvo vedomostí. Ale doteraz nemali dobrý spôsob, ako sa spolu spojiť. Od tohto prvého - spojme sa, začali sa ponúkať všetky druhy možností.

Všeobecná zhoda bola v tom, že ak aj ľudia, ktorí majú vysoko rýchlostný prístup k Net-u, sú ochotní ho zdieľať s tými, ktorí ho chcú, ale z rôznych príčin ho nemôžu dostať, má to niekoľko technických prekážok, ktoré je potrebné prekonať:

- Riešenie nemôže stáť tisíce dolárov, inak si ho nikto nebude môcť dovoliť.
- Musí byť bezpečný a jednoduchý spôsob zistenia kto je kto a obmedzenia čo môžu užívatelia robiť na sieti (takže vlastníci uzlov by nemali byť vystavený zloduchom, alebo že si ich ťažko zarobenú šírku pásma privlastní voľne sťahujúca skupinka).
- Riešenie musí byť dostatočne jednoduché na nastavenie pre niekoho s malými skúsenosťami a malo by vyžadovať malú, alebo žiadnu údržbu.
- Musí byť ľahký spôsob, ako sa ľudia zaujímajúci o spoje z bodu do bodu navzájom stretnú.
- Ľudia, ktorí majú priemerné vedomosti ako pokračovať, potrebujú prístup ku všetkým druhom informácií, od výberu mikrovlnných konektorov, po konfiguráciu laptopov.

Mali sme nejaké odpovede na tieto otázky, ale bolo jasné, že to budú dlhotrvajúce problémy, zdieľané každým, kto sa bude pokúšať dať dohromady komunitnú skupinu. Na NoCat sme dali toľko informácií, koľko sme mohli a obrátili sme sa na ostatných, ktorí mali odpovede.

Najbližšia bezdrôtová komunitná skupina ku Sebastopol-u bola BAWUG, ktorá sa pravidelne stretávala v oblasti San Jose. Aj keď sme očividne pracovali vedľa seba, zdalo sa, že nastal čas pozrieť sa, čo naši severní susedia robili. Zobral som pár nadšencov a vybrali sme sa spolu na dvojhodinovú púť do San Jose, na stretnutie.

Stretnutie BAWUG v júni 2001 bolo ohromnou príležitosťou pre budúcu sieť. Veľmi podobne ako na našom stretnutí v Sebastopol-e, boli tam ľudia s úplne rozdielnymi schopnosťami i očakávaniami (len tu ich bolo okolo päťdesiat!). Po pár zaujímavých prednáškach som dostal možnosť pohovoriť si s anténnymi guru, nejakými Apple AirPort hackermi a dokonca s komerčným bezdrôtovým poskytovateľom.

Bolo tam veľa vzrušenia okolo blížiaceho sa stretnutia Portland Summit. Zovšadiaľ sa lídri bezdrôtových komunít chystali stretnúť v Portlande, na víkend plný plánovania, rozhovorov, piva a všeobecného hackerstva. Bolo to stretnutie, ktoré som nemohol zmeškať.

9.1.7 Summit v Portlande

Minulý jún, vôbec po prvý krát, ľudia z komunitných bezdrôtových sietí z celej krajiny (a dokonca z Kanady!) sa stretli v Portlande, aby sa porozprávali o tom, kam smerujeme. Boli tam organizátori zo Seattlu, New Yorku, Britskej Kolumbie, Portlandu, oblasti San Franciského zálivu a Sebastopolu. Strávili sme pár veľmi produktívnych dní, zastrešujúcich netradičné témy, ako je konštrukcia antén, schémy sietí, FCC a „catch and release“ portál. Bolo tam veľa energie a priazne medzi skupinami, všetky experimenty sme uskutočňovali spolu (prirodzene, pivo snáď tiež trochu pomohlo).

Myslím si, že Portlanský summit bol veľmi povzbudzujúci pre všetkých. Mali sme tam ľudí z celého sveta, ktorí zdieľali niečo zo spoločnej vízie: neobmedzenú slobodnú šírku pásma všade. Rozvinuli sme túto myšlienku nezávisle a hoci niektoré detaily, ako sa o to pokúšame, sa rôznia, konečný zámer je rovnaký. Bezdrôtový komunitný sieťový prístup sa zdá byť nápad, ktorého čas konečne prišiel, hardvér, softvér a chrbticová sieť sa stávajú lacnými a dostatočne všadeprítomnými na to, aby sa to podarilo. Všetky naše skupiny chcú posilniť naše miestne komunity prinesením sieťového prístupu každému, kto sa usiluje byť toho súčasťou. A spoluprácou, zdieľaním toho čo sme sa naučili, produkovaním softvéru a podieľaním sa na spoločnom úsilí zistíme, že dokážeme dosiahnuť tento cieľ rýchlejšie, než skúšaním nájsť riešenie samostatne.

9.1.8 Budúcnosť

Teraz, s približne 150 ľuďmi v diskusnej skupine, pravidelnými mesačnými stretnutiami a dokonca narastajúcim počtom uzlov s verejným prístupom sa definitívne približujeme všadeprítomnému slobodnému sieťovému prístupu pre každého, kto to chce používať. Softvér NoCatAuth bol oficiálne vypustený (detaily viď <http://nocat.net/>) a teraz je prioritou v Sebastopol-e dostať uzly online.

Spoločným úsilím a s bezdrôtovou technológiou sa Internet rýchlo stáva viac a viac všadeprítomným. Na základe mojej priamej skúsenosti s ľuďmi pracujúcimi na tomto projekte, som našiel dôležitý spoločný prvok: voľný prístup k informáciám je vždy žiadaný a bariéry proti tomuto prístupu spôsobujú bolesť. Verím, že práca na poskytnutí voľného, neobmedzeného prístupu do Internetu je osožná nie len pre jednu miestnu komunitu, ale tiež pre celý svet. Dúfam, že táto kniha Vám pomohla uskutočniť Vaše zámery a pomohla Vám lepšie sa pripojiť k Vašej miestnej komunite.

Príloha

A.1 Výpočet straty cestou (Path Loss Calculations)

Tu je jednoduchá tabuľka vypočítaných strát cestou vo voľnom priestore pre kanály 1 a 11, pri čistej priamej viditeľnosti. Ako použiť tieto čísla na zistenie toho, ako ďaleko dosiahne Vaša sieť si pozrite [kapitolu 6](#). Vzdialenosti sú v míľach a straty v dB.

Vzdialenosť (míle)	2.412GHz (kanál 1)	2.462GHz (kanál 11)
0.5	98.2	98.4
1	104.2	104.4
2	110.3	110.4
3	113.8	114.0
4	116.3	116.5
5	118.2	118.4
7	121.1	121.3
10	124.2	124.4
15	127.8	127.9
20	130.3	130.4
25	132.2	132.4
30	133.8	134.0

Táto tabuľka strát cestou bola vypočítaná podľa nasledujúceho vzorca, zaokrúhlená na desatiny:

$$L = 20 \log(d) + 20 \log(f) + 36.6$$

Snáď najspoľahlivejší zdroj informácií o rádiách na svete nájdete online na ARRL <http://www.arrl.org/>, alebo si pozrite niektorú z ich výborných kníh (osobitne ich *UHF/Microwave Experimenter's Manual and Antenna Book* je rozhodne zdroj pre učenie sa o mikrovlnnej komunikácii).

A.2 Odkazy na stránky bezdrôtových komunit

Fenomén bezdrôtových komunit je badať na celom svete. Dobrý zoznam projektov je na <http://www.toaster.net/wireless/community.html>. Zopár väčších sietí (a náš skromný Sebastopol) je uvedených nižšie. Ak vo Vašej oblasti nie je komunitná skupina, založte nejakú Vy! Bol som naozaj prekvapený širokým okruhom ľudí zaujímajúcich sa o komunikáciu. Vypusťte slovo, spustite diskusnú skupinu a spojte sa s Vašou komunitou. Prostriedky, ktoré dokáže dať dokopy komunita, pre spoločný projekt, sú ohromujúce. Jednoducho to musíte urobiť!

Seattle Wireless (Seattle, WA)

<http://seattlewireless.net/>

Bay Area Wireless Users Group (San Francisco Bay, CA)

<http://www.bawug.org/>

Personal Telco Project (Portland, OR)

<http://www.personaltelco.net/>

NYC Wireless (New York, NY)

<http://www.nycwireless.net/>

GBPPR (Green Bay, WI)

<http://www.gsl.net/n9zia/index.htm>

Guerrilla.Net (Cambridge, MA)

<http://www.guerrilla.net/>

NoCat (Sebastopol, CA)

<http://nocat.net/>

A.3 FCC Part 15 Rules

Predpis, vzťahujúci sa na nelicencované pásmo 2.4GHz, platný v USA. Pozri originálny text knihy.

Úplné znenie Part 15 je online na:

<http://www.access.gpo.gov/nara/cfr/cfr-table-search.html>

Kvalitná diskusia o predpisoch vzťahujúcich sa na 802.11b je online na:

http://www.lns.com/papers/FCCPart15_and_the_ISM_2.4G_Band.index

A.4 Jednoduché spravovanie schém

Tu je jednoduchá metóda spravovania Vašich sieťových schém na Linuxe. Budete potrebovať, mať nainštalované *sudo* a privilégia pre *sudo* na spustenie */sbin/cardctl*.

Vytvorte nasledujúci shell skript nazvaný *scheme*:

```
#!/bin/sh

SCHEME=`/usr/bin/basename $0`

if [ "$SCHEME" == "scheme" ]; then
    unset SCHEME
fi

/usr/bin/sudo /sbin/cardctl scheme $SCHEME
```

Nainštalujte tento skript niekde do Vašej PATH (ja som svoj umiestnil do *~/bin*). Potom vytvorte symbolické linky na daný skript, s menami schém, ku ktorým chcete mať rýchly prístup, v tom istom adresári:

```
rob@entropy:~/bin$ ln -s scheme home
rob@entropy:~/bin$ ln -s scheme oreilly
rob@entropy:~/bin$ ln -s scheme nocat
rob@entropy:~/bin$ ln -s scheme any
```

Teraz urobte zodpovedajúce odseky vo Vašom */etc/pcmcia/wireless.opts*:

```
home, *, *, *)
    INFO="IBSS net at Home"
    ESSID="HomeNet"
    MODE="Ad-Hoc"
    KEY="1234-5678-90"
    RATE="11M"
    ;;

oreilly, *, *, *)
    INFO="Work"
    ESSID="OReillyNet"
    MODE="Managed"
    KEY="s:SHHHH"
    IWCONFIG="power unicast"
    ;;

nocat, *, *, *)
    INFO="NoCat Community net"
    ESSID="NoCat"
    MODE="Managed"
    ;;

any, *, *, *)
    INFO="Default configuration"
    ESSID="ANY"
    MODE="Managed"
    ;;
```

Teraz, keď chcete zmeniť schému rýchlo, len napíšete *home*, alebo *any*, aby ste okamžite zmenili všetky Vaše bezdrôtové a sieťové nastavenia. Ako osobitný prídavok, napísanie *scheme*, zobrazí aktuálnu schému. Majte na pamäti, že *sudo* Vás vyzve na zadanie hesla, takže potrebujete byť root, aby ste zmenili schému.

Tiráž

Náš vzhľad je výsledkom pripomienok čitateľov, našich vlastných experimentov a odozvy z distribučných kanálov. Charakteristický obal dopĺňa náš osobitý postoj k technickým témam, meniť osobnosť a život na obvyčajný predmet.

Zviera na obale knihy *Building Wireless Community Networks* je Carolina parakeet (malý, žiarivo farebný vták s dlhým chvostom), *Conuropsis carolinensis*, jediný papagáj, ktorý sa prirodzene vyskytuje v USA. Tento stopu dlhý, viacfarebný vták, so zeleným telom a žltó-oranžovou hlavou a nohami, bol pažravý jedák ovocia a obilných semien, vedený k hromadnej záhube ako poľnohospodársky škodca. Hoci sa voľakedy nachádzal na celom juhovýchode USA, posledný známy Carolina parakeet zahynul v zoo v Cincinnati, 21 februára 1918.

Na tvorbe knihy sa podieľali: Leanne Soylemez - redaktor, Catherine Morris - copyeditor, Mary Anne Weeks Mayo - kontrola kvality, Joe Wizda - napísal index.

Ellie Volckhausen navrhol obal tejto knihy podľa námetu, ktorý vytvoril Edie Freedman. Obrázok na obale je rytina z 19. storočia z Dover Pictorial Archive. Emma

Colby realizovala grafickú úpravu obalu pomocou Quark™XPress 4.1 s použitím fontu ITC Garamond od Adobe.

David Futato navrhol vnútornú úpravu. Mihaela Maier konvertovala súbory z Microsoft Word do FrameMaker 5.5.6, použitím nástrojov, ktoré vytvoril Mike Sierra. Použité sú textové fonty Linotype Birka, Adobe Myriad Condensed, LucasFont's TheSans Mono Condensed. Ilustrácie, ktoré sa nachádzajú v knihe vytvoril Robert Romano a Jessamyn Read použitím Macromedia FreeHand 9 a Adobe Photoshop 6. Ikony tip a varovanie nakreslil Christopher Bing. Tiráž napísal Leanne Soylemez.

Pár poznámok k prekladu

Tento preklad som realizoval ako môj príspevok k myšlienke projektu SKFREE a je k dispozícii pre všetkých členov SKFREE zdarma.

Dúfam, že pomôže všetkým, ktorí sa zaujímajú o výstavbu bezdrôtových sietí (no originálny text im robí problémy) a nie je im cudzia myšlienka spolupracujúcej komunity.

Snahou bolo zachovať originálnu grafickú úpravu, pričom text je len prekladom, uvedené sú reálie USA, bez akýchkoľvek úprav. Knihu by určite bolo možné vylepšiť informáciami z oblasti topografických máp na Slovensku, prevodom dĺžkových mier na metrické, diskusiou o u nás platných zákonoch namiesto FCC 15, aktuálnymi cenami v SKK a pod. Mnoho z uvedeného je však možné nájsť online na portále www.skfree.net, napr. článok venovaný konektorom je možno ešte podrobnejší ako text knihy.

Preklad je len amatérsky, ale pre tých, ktorí vôbec nevedia anglicky bude snáď užitočný. Vopred prosím, ospravedlňte moju slabú znalosť gramatiky a štylistiky a tiež zníženú kvalitu obrázkov. V prípade akýchkoľvek pochybností prosím konzultujte originálny text.

Rovnako, ako mnoho veľkých firiem, ani ja za nič neručím ;-) a tak za prípadne škody súvisiace s použitím tohto prekladu si môžete sami.