Univerzita Palackého v Olomouci

Pedagogická fakulta

Technologie bezdrátových sítí

základní principy a standardy

doc. PhDr. Milan Klement, Ph.D.

Olomouc 2019

Obsah

ÚVOD 4
1 Teoretické základy standardu IEEE 802.11 5
1.1 Základní pojmy 5
1.1.1 Standard IEEE802.11b a WiFi 6
1.2 Frekvenční rozsahy IEEE802.11b 6
1.3 Standard 802.11 – a co ty písmenka za číslem? 8
2 Struktura sítě WLAN 12
2.1 Komponenty sítě WLAN 12
2.2 Typy bezdrátových sítí 13
2.3 Fyzická vrstva bezdrátové sítě 802.11 16
2.4 Linková (MAC) vrstva bezdrátové sítě 802.11 18
2.5 Architektura bezdrátové sítě 802.11 20
3 Hardware pro WiFi sítě – Access pointy 23
3.1 Obecně o zařízeních WiFi sítě 23
3.2 Access Points (AP) 24
3.3 Co všechno další může AP umět 25
3.4 Zabezpečení AP a WLAN 28
3.5 Režimy provozu AP 30
3.5.1 Režim Router 31
3.5.2 Režim Home Gateway 32
3.5.3 Režim Access Point 33
4 Hardware pro WiFi sítě – Antény 36
4.1 Jak daleko "vidí" bezdrátové sítě 36
4.2 Ztráty na trase a antény bezdrátových sítí 38
4.3 Typy antén 41
4.3.1 Všesměrové antény 42
4.3.2 Sektorové antény 42
4.3.3 Směrové antény 43
4.4 Základní parametry antén 44
4.4.1 Zisk 44
4.4.2 Vyzařovací úhly a diagramy 45
4.4.3 Polarizace 45
4.4.4 Jak si vybrat správnou anténu? 46
5 Hardware pro WiFi sítě – Konektory, kabely a bleskojistky 50
5.1 Konektory 50
5.2 Kabely 52
5.3 Bleskojistky 54
Použitá literatura 57

ÚVOD

O tomto století se hovoří jako o století informace. Informace se stává hlavním zdrojem vědeckého i sociálního rozvoje společnosti. Ještě před několika lety bylo pro nás nepředstavitelné, že svět bude ovládán pomocí počítačů. Dnes už si život bez nich nedokážeme představit.

Z toho důvodu vznik i tento výukový text, který je určen všem zájemcům, kteří se chtějí naučit konfigurovat a ovládat bezdrátové rádiové sítě, postavené na technologii Wi-Fi. Předložený studijní materiál Vás tedy postupně seznámí se základy hardware tohoto typu počítačových sítí a základními principy jejich fungování. Rozsah témat je volem tak, aby Vám umožnil orientovat se v oblasti bezdrátových počítačových sítí. Pokud tedy budete společně s námi sledovat následující výklad, získáte mnoho teoretických i praktických znalostí a dovedností, které Vám umožní rychlou a efektivní správu bezdrátové počítačové sítě.

Po prostudování tohoto materiálu budete schopni:

- charakterizovat a vysvětlit základní pojmy týkající se problematiky bezdrátových sítí,
- uvést jednotlivé typy bezdrátových přenosů,
- vymezit a popsat technologií bezdrátových sítí postavených na struktuře přístupových bodů (AP),
- vymezit a popsat technologií bezdrátových sítí postavených na struktuře ad-hoc,
- popsat jednotlivé hardwarové prvky bezdrátové sítě postavené na technologii WiFi.

A nyní několik pokynů ke studiu.
Budeme s Vámi rozmlouvat prostřednictvím tzv. průvodce studiem. Odborné poznatkové penzum najdete v teoretických pasážích, ale nabídneme Vám také cvičení, pasáže pro zájemce, kontrolní úkoly, shrnutí, pojmy k zapamatování a studijní literaturu. Je vhodné, ale ne nezbytně nutné, abyste tento text studovali především u Vašeho osobního počítače a všechny popsané postupy ihned aplikovali. Také jsme pro vás připravili mnoho kontrolních úkolů, na kterých si ihned ověříte, zda jste nastudovanou problematiku pochopili a zda jste schopni ji aplikovat.
Proto je v textu umístěno mnoho obrázků, které Vám umožní rychlou a snadnou orientaci ve výkladu. Tyto obrázky obsahují skutečné zobrazení síťových komponent, počítačových komponent, uživatelských rozhraní aplikací apod. U každého takového obrázku je potom umístěna příslušná legenda (zpravidla ihned pod obrázkem), která daný označený objekt nebo prvek popisuje a vysvětluje také jak je možné jej ovládat. Proto je vhodné nejprve daný obrázek (který vždy vysvětluje danou problematiku) prohlédnout, podle orientační značky identifikovat popisované prvky nebo objekty a poté si přečíst příslušnou legendu. Dále je text doplněn o další grafické znaky (ikony), které Vám usnadní orientaci v textu. Tyto ikony se nacházejí v popisném sloupci, který je umístěn na okrajích textu.

Vážení přátelé, přejeme Vám mnoho úspěchů při studiu a trpělivost při získávání poznatků o struktuře a fungování bezdrátových počítačových sítí.

Autor

1 Teoretické základy standardu IEEE 802.11

Cíle

Po prostudování této kapitoly byste měli být schopni:

- umět vysvětlit základní pojmy z oblasti bezdrátových sítí,
- definovat standard IEEE 802.11

Průvodce studiem

Hned na začátku tohoto textu Vás zaskočíme několika řádky teorie. Nedejte se prosím tímto odradit, protože po prostudování této kapitoly budete schopni vysvětlit několik základních a velmi důležitých pojmů, které jsou podstatné pro další studium.
Dáme Vám dobrou radu. Je neefektivní důležité pasáže textu opakovaně pasivně pročítat s domněním, že Vaše vědomosti poté budou trvalé. Je vhodné pokoušet se vysvětlit studovanou oblast vlastními slovy a provádět si zestručňující výpisky. Jistě ale naleznete takovou metodu učení, která Vám bude nejvíce vyhovovat. Takže s chutí do toho!!!

Vstupní znalosti a podmínky:

- V této i dalších kapitolách nemusíte mít žádné vstupní znalosti. Předpokládáme totiž, že jste v oblasti bezdrátových sítí naprostými laiky či úplnými začátečníky. Proto je výklad koncipován tak, abyste získali všechny potřebné znalosti a dovednosti přímo při studiu tohoto materiálu.

Potřebný čas pro studium kapitoly:

- 60 minut

1.1 Základní pojmy

Většina z vás si asi již odpověděla na otázku, proč se o bezdrátové sítě zajímat. Instalace bezdrátových sítí je na jednu stranu jednodušší na výstavbu a technickou realizaci, protože není třeba pokládat žádnou kabeláž, na stranu druhou nabízejí bezdrátové sítě podstatně nižší rychlosti, než nejmodernější Ethernetové kabelové sítě. Jenže pokud nezamýšlíte přenášet ve vaší síti obrovská kvanta dat najednou, mohou výhody bezdrátové sítě převážit.

Smyslem této kapitoly je dát Vám kompendium základních znalostí o bezdrátových sítích. Konkrétněji se budeme bezdrátovými sítěmi zabývat v následujících kapitolách, tato kapitola je spíše takovým průřezem toho, co byste měli vědět.

IEEE 802.11

Bezdrátové sítě (**WLAN – Wireless Local Area Network**) nabízejí v principu podobné služby a flexibilitu, jako sítě drátové. Je možné zapojovat do nich servery a jejich klienty, ale také je možné v nich vytvářet spojení peer-to-peer. Z hlediska funkčnosti a výsledku jsou, odhlédneme-li od dosahovaných přenosových rychlostí, ekvivalentní k sítím drátovým, kupříkladu Ethernetu. Zásadně se samozřejmě liší ve své skutečné podstatě, v tom, jak fungují.

Bezdrátové sítě existují od roku 1992, tehdejší zařízená ale pracovala na provozních rychlostech hluboko pod 1 Mbps. V té době také chyběl jakýkoliv standard, takže jste museli používat síťové prvky

stejného výrobce. Tato situace se významně zlepšila po přijetí standardu **IEEE 802.11**, jímž jsou moderní **WLAN** sítě také definovány a standardizovány.

1.1.1 Standard IEEE802.11b a WiFi

Když se dnes hovoří o bezdrátových sítích, s oblibou se míchá několik zkratek dohromady. Zkusme si ten zmatek trochu ujasnit.

- Prvním důležitým pojmem je zkratka **WLAN**. Tato zkratka **Wireless Local Area Network** označuje obecně jakoukoliv bezdrátovou síť a je vlastně ekvivalentní zkratce LAN. Jakákoliv bezdrátová síť kde figurují počítače se tedy odborně říká WLAN. WLAN

- Dalším termínem je **IEEE802.11b**. Tento pojem představuje označení standardu standardizačního institutu IEEE – jde o standard definující bezdrátové sítě v nelicencovaném pásmu 2,4 GHz. Dlužno podotknout, že místo písmenka B na konci můžete najít i další písmenka – tím je zpravidla odlišena jiná verze standardu a zpravidla také i skutečnost, že tento derivát standardu IEEE802.11 pracuje na jiné frekvenci. Přehled těchto derivátů a písmenek si za chvíli představíme v tabulce. IEEE 802.11b

- Poslední nyní důležitý pojem je zkratka **WiFi – Wireless Fidelity**. Tato zkratka se často zaměňuje s výrazem IEEE802.11b. Jde totiž o označení a logo udělované výrobkům pracujícím podle standardu 802.11b, které jsou mezi sebou vzájemně propojitelné. Výrobky označené WiFi tedy můžete vcelku bez obav propojovat s jinými výrobky označenými logem WiFi od jiných výrobců. Ovšem není to výlučné označení – o toto označení si musí výrobce požádat a ačkoliv jej dnes již většina výrobků nese, při dodržení standardu byste neměli mít problémy i s neoznačenými výrobky. Pravdou ale je, že právě WiFi označení dává značnou záruku propojitelnosti. Výrobci tak reagovali na problémy s prvními sériemi výrobků pracujícími dle standardu 802.11b, kdy mezi sebou často nebylo možné jednotlivé výrobce a výrobky kombinovat. To samozřejmě vedlo k nedůvěře uživatelů a k jejich nezájmu o bezdrátové sítě. Pokud budeme tedy napříště hovořit o IEEE802.11b, budeme označení WiFi používat jako ekvivalent tomuto standardu, protože jde přeci jen o zapamatovatelnější a lidštější název a výše uvedená výhrada interoperability již dnes ztratila právě rozšířením a akceptací interoperability mezi zařízeními výrobců na důležitosti. Zpravidla se tedy označení IEEE802.11b používá tam, kde se mluví o standardu, zatímco pojem WiFi se používá v případě, když se mluví o zařízení pracujících podle standardu. Toho se také budeme držet. WiFi

Úkol číslo 1

Co znamená zkratka WiFi?

1.2 Frekvenční rozsahy IEEE802.11b

Bezdrátové sítě standardu **IEEE802.11b** pracují ve frekvenčním pásmu **2,4 – 2,4835 GHz**, tedy zjednodušeně řečeno v pásmu **2,4 GHz**. Toto pásmo se také často označuje jako **ISM**, tedy **Industrial, Scientific, Medical**. V tomto nelicencovaném pásmu pracuje mnoho různých bezdrátových zařízení, například bluetooth produkty, ale i mikrovlnné trouby a v zahraničí i bezdrátové telefony (u nás jejich provoz není povolen). Hodně se spekuluje o tom, jak provoz mikrovlnek ovlivňuje WiFi zařízení – budeme se tomu věnovat někdy speciálně, protože je to docela zajímavé, kolik nesmyslných mýtů o tom existuje. Pásmo 2,4 GHz

Frekvenční rozsah se ovšem liší země od země – v některých státech není povolené plné frekvenční spektrum, protože již jsou jeho části využívány pro jiné účely. Pro nás je příjemné, že **ČTÚ** (Český Rádiové frekvence

telekomunikační úřad) povoluje plné frekvenční spektrum, jako je tomu v USA nebo ve většině Evropy, takže výrobky koupené v USA můžete vcelku s klidným svědomím v ČR používat.

Povolené radiové frekvence:

Region	Frekvenční rozsah v GHz	Počet kanálů
USA	2,4000 – 2,4835	79
Evropa	2,4000 – 2,4835	79
Francie	2,4465 – 2,4835	27
Španělsko	2,445 – 2,475	35
Japonsko	2,471 – 2,497	23

IEEE 802.11a

Zároveň s boomem WiFi zařízení se na trh pomalu dostávají zařízení postavená na standardu **IEEE 802.11a** a pracující v pásmu **5GHz**. Pro ně se prosazuje označení WiFi5. Jejich hlavní výhodou je vyšší rychlost, kterou jsou schopná přenášet data – až 54 Mbps. Na druhou stranu mají ale nižší dosah a větší náchylnost na rušení. Navíc v ČR není možné je používat mimo budovy.

IEEE 802.11b,g

Zatímco pro standard **802.11b** a **802.11g** je vyhrazeno pásmo **2,4 GHz**, u standardu **802,11a** se pásmo souhrnně označuje jako pásmo **5 GHz**. To vyhrazené pásmo je podstatně větší než **ISM** pásmo **2,4 GHz**, bohužel ale dosud nedošlo ke shodě mezi americkým regulátorem FCC a evropským regulačním orgánem EU o společném postupu při uvolňování a využívání pásma 5 GHz.

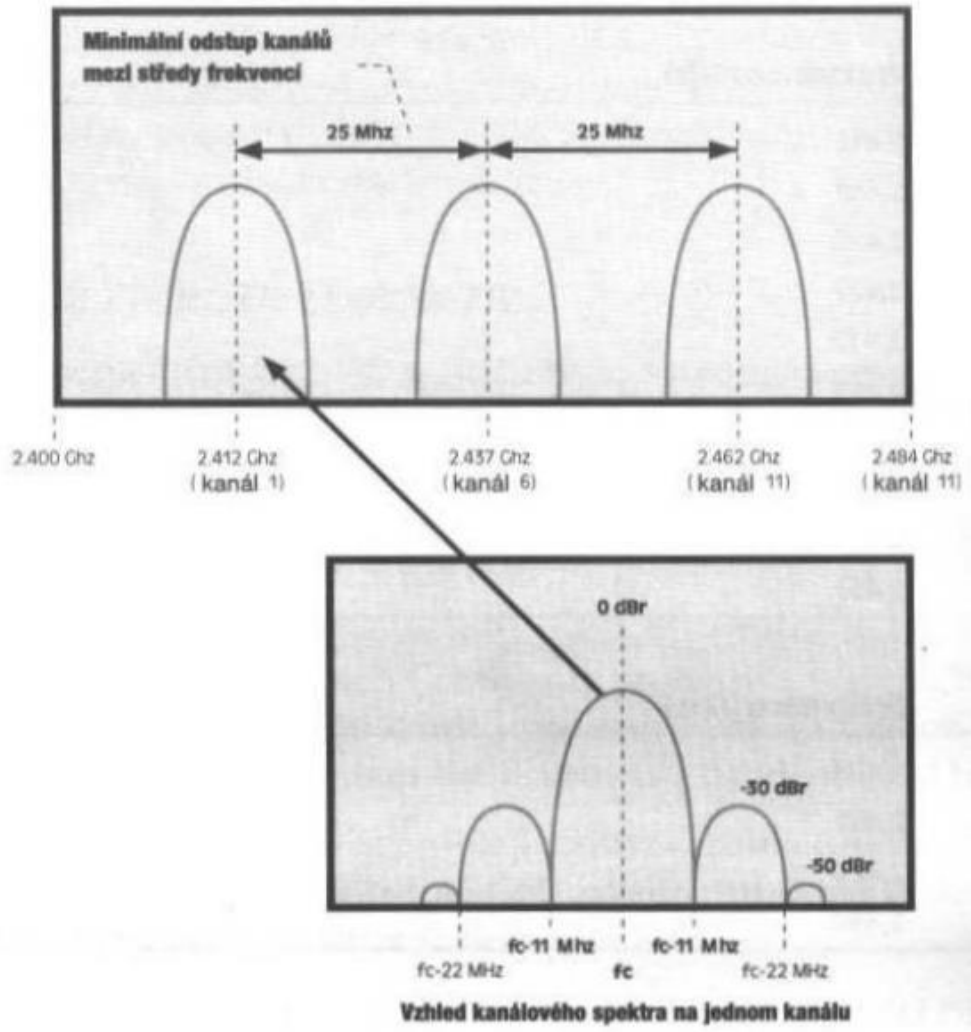
V případě standardu **802.11b** a **802.11g** jde o následující frekvence. Rozdělení do kanálů je platné pro častěji používané rozprostřené spektrum, systémy s frekvenčními proskoky si dělí celé spektrum do 79 (75) kanálů. Označením frekvence se rozumí střed frekvence.

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

Česká republika (přidržujíc se konvence ETSI) má k dispozici největší počet povolených kanálů. Jenže ani magické číslo 13 není nijak moc. Bohužel to neznamená, že je k dispozici 13 plnohodnotných frekvencí, neboť technologie rozprostřeného spektra znamená vysílání do frekvenčního rozsahu **22 MHz**. Jenže odstup mezi kanály je pouze **5 MHz**, tedy vysílání na jednom kanálu se překrývá s vysíláním na sousedních čtyřech kanálech.

Pokud chcete provozovat dva přístupové body tak, aby se jejich signál překrýval a nerušil, musíte je nastavit tak, aby pracovaly minimálně 5 kanálů od sebe.

Co si pod tím máte představit, vidíte na obrázku:



1.3 Standard 802.11 – a co ty písmenka za číslem?

Standard **802.11** vznikl v roce **1992** a definoval bezdrátovou síť v pásmu **2,4 GHz** a o rychlostech 1 nebo 2 MHz. Protože však postupem doby vznikaly další a další nároky na posun tohoto standardu, vznikaly v rámci této pracovní skupiny další pracovní podskupiny věnované rozšířením a změnám v tomto standardu. IEEE 802.11

Tyto skupiny jsou označované písmeny, které se přidávají za číslo standardu 802.11. Poslední standard IEEE 802.11 byl publikován v roce 1999 a je zdarma dostupný na stránkách www.ieee.org. Novější revize standardu zatím nebyla vydána a jsou pouze ve fázi rozpracování, diskuse nebo schvalování.

Tak a nyní si můžeme nyní rekapitulovat všechna ta písmenka za jedenáctkou:

Typy normy IEEE 802.11

- **802.11a** – WLAN v pásmu 5 GHz a s rychlostí až 54 Mbps.
- **802.11b** – WLAN v pásmu 2,4 GHz a s rychlostí až 11 Mbps.
- **802.11b-cor** – úpravy MIB v 802.11b (MIB = Management Information Base), v diskusi
- **802.11c** – definice procedur pro síťové mosty, bridge. Ve skutečnosti s to WLAN má jen málo společného, jde ale o užitečný standard pro Access Pointy.
- **802.11d** – Mezinárodní harmonizace. Se vznikem standardu 802.11 se ukázalo, že je potřeba mezinárodní kooperace a harmonizace. Zejména pásmo 5 GHz se používá v mnoha státech různě a bylo třeba tomu standardizaci přizpůsobit tak, aby nevycházela vstříc pouze potřebám USA a Japonska. To měla za úkol tato pracovní skupina.
- **802.11e –** rozšíření MAC pro QoS – Zkratka QoS označuje službu Quality of Service zajišťující vyrovnanou kvalitu služby důležitou například pro multimédia. Zjednodušeně řečeno je potřeba, aby když někdo v bezdrátové síti telefonuje nebo pořádá videokonferenci, aby trvalý tok jeho dat měl přednost před lidmi, kteří například jen stahují poštu a chvilkový výpadek naprosto nepoznají, zatímco v hlasu nebo videu by byl hodně poznat. Toto upřednostnění určitých dat v bezdrátové síti má přinést MAC, Medium Access Layer. To upřednostní hlasové a videopřenosy. Finalizace tohoto standardu má být do konce roku 2002 a v polovině roku 2003 by mohly být dostupné produkty podporující MAC (rozhodně neplést s MAC adresami!). Mělo by být možné všechny Access Pointy upravit updatem firmware tak, aby splňovaly tento standard.
- **802.11f** – Inter Access Point Protocol (IAPP) – Stávající specifikace 802.11 nezahrnují standardizaci komunikace mezi jednotlivými Access pointy pro zajištění bezproblémového roamingu, tedy přechodu uživatele od jednoho Access pointu k druhému. V současné době tak produkty různých výrobců nejsou schopny spolu o roamingu bezproblémově komunikovat a při výstavbě větších sítí, kde se roaming předpokládá, je nutno používat Access pointy jednoho výrobce s jejich proprietárním řešením, nebo celou záležitost řešit úplně mimo Access pointy.
- **802.11g** – zvýšení rychlosti v pásmu 2,4 GHz na 20 Mbps se zpětnou kompatibilitou s 802.11b.
- **802.11h** – změny v řízení přístupu k spektru 5GHz, které by měly reflektovat připomínky regulátorů evropských zemí tak, aby bylo možno sítě v pásmu 5 GHz využívat i mimo budovy.
- **802.11i** – zlepšení bezpečnosti v 802.11 bezdrátových sítích vylepšením autentifikačního a šifrovacího algoritmu.
- **802.11j** – práce na alokaci nových frekvenčních rozsahů pro multimediální služby bezdrátových sítí. Jde o vysoké frekvence a ještě chvíli potrvá, než uvidíme první výrobky.
- **802.11k** – tento projekt má definovat měření a správu radiových zdrojů tak, aby vyhovovaly novým vysokofrekvenčním radiovým sítím. Vlastně pokračování práce 802.11j.

Zde můj přehled o písmenkách končí a ostatně jak vidíte, v praxi si vystačíme s písmenky B pro WiFi, s písmenkem A pro WiFi5 a s písmenkem G pro zvýšení rychlosti WiFi.

Pokud by vás zajímalo, proč se novější standard označuje jako 802.11a zatímco starší je označen jako b, pak vysvětlení je prosté – standard 802.11a je ve skutečnosti starší, ale technicky byl náročnější na implementaci do výrobků, takže výrobky s WiFi5 přicházejí na trh později, než jejich WiFi bratříčkové.

Úkol číslo 2

V kterém roce vznikl standard 802.11?

Shrnutí

- Bezdrátové sítě (**WLAN – Wireless Local Area Network**) nabízejí v principu podobné služby a flexibilitu, jako sítě drátové. Je možné zapojovat do nich servery a jejich klienty, ale také je možné v nich vytvářet spojení peer-to-peer.

- Bezdrátové sítě existují od roku 1992, tehdejší zařízená ale pracovala na provozních rychlostech hluboko pod 1 Mbps. V té době také chyběl jakýkoliv standard, takže jste museli používat síťové prvky stejného výrobce.
- **WLAN** – tato zkratka **Wireless Local Area Network** označuje obecně jakoukoliv bezdrátovou síť a je vlastně ekvivalentní zkratce LAN. Jakákoliv bezdrátová síť kde figurují počítače se tedy odborně říká WLAN.
- **IEEE802.11b** – tento pojem představuje označení standardu standardizačního institutu IEEE, kdy jde o standard definující bezdrátové sítě v nelicencovaném pásmu 2,4 GHz.
- **WiFi – Wireless Fidelity** – tato zkratka se často zaměňuje s výrazem IEEE802.11b. Jde totiž o označení a logo udělované výrobkům pracujícím podle standardu 802.11b, které jsou mezi sebou vzájemně propojitelné. Výrobky označené WiFi tedy můžete vcelku bez obav propojovat s jinými výrobky označenými logem WiFi od jiných výrobců.
- Bezdrátové sítě standardu **IEEE802.11b** pracují ve frekvenčním pásmu **2,4 – 2,4835 GHz**, tedy zjednodušeně řečeno v pásmu **2,4 GHz**. Toto pásmo se také často označuje jako **ISM**, tedy **Industrial, Scientific, Medical**.
- Zároveň s boomem WiFi zařízení se na trh pomalu dostávají zařízení postavená na standardu **IEEE 802.11a** a pracující v pásmu **5GHz**. Pro ně se prosazuje označení WiFi5.
- Česká republika (přidržujíc se konvence ETSI) má k dispozici největší počet povolených kanálů. Jenže ani magické číslo 13 není nijak moc. Bohužel to neznamená, že je k dispozici 13 plnohodnotných frekvencí, neboť technologie rozprostřeného spektra znamená, vysílaní do frekvenčního rozsahu **22 MHz**. Jenže odstup mezi kanály je pouze **5 MHz**, tedy vysílání na jednom kanálu se překrývá s vysíláním na sousedních čtyřech kanálech.
- Pokud chcete provozovat dva přístupové body tak, aby se jejich signál překrýval a nerušil, musíte je nastavit tak, aby pracovaly minimálně 5 kanálů od sebe.
- Standard **802.11** vznikl v roce **1992** a definoval bezdrátovou síť v pásmu **2,4 GHz** a o rychlostech 1 nebo 2 MHz. Protože však postupem doby vznikaly další a další nároky na posun tohoto standardu, vznikaly v rámci této pracovní skupiny další pracovní podskupiny věnované rozšířením a změnám v tomto standardu.

Kontrolní otázky a úkoly

1. Vysvětlete pojem IEEE 802.11.
2. Vysvětlete pojem bezdrátová síť.
3. Vysvětlete pojem WiFi.
4. Vysvětlete pojem WLAN.

Pojmy k zapamatování

IEEE, IEEE 802.11, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, WiFi, WLAN, frekvenční pásmo, komunikační kanál.

Literatura

Základní:

ZANDL, P. *WiFi – praktický průvodce.* 1. vyd. Brno: Vydavatelství Computer Press, 2003. 217 s. ISBN 80-7226-632-2.

KÖHRE, T. *Stavíme si bezdrátovou síť Wi-fi* [překlad Marek Šiller]. Vyd. 1. vyd, Brno: Vydavatelství Computer Press, 2004. 295 s. ISBN 80-251-0391-9.

Rozšířená (pro hlubší pochopení):

DAVIS, H. *Průvodce úplného začátečníka pro Wi-Fi bezdrátové sítě: není zapotřebí žádných předchozích zkušeností!* [přeložil Karel Voráček]. 1. vyd. Praha: Vydavatelství Grada, 2006. 334 s. ISBN 80-247-421-3.

Průvodce studiem

Tato kapitola asi pro většinu z Vás zajímavá nebyla, že? Pokud jste ale studovali pečlivě, udělali jste velký kus práce, který se Vám zhodnotí v dalším studiu. A navíc, konečně již přesně víte, co je to ten WLAN, WiFi a frekvenční pásmo. Narazíte-li v budoucnu na neznámý pojem, není nic jednoduššího, nežli si jeho obsah nalézt v některém z výkladových slovníků výpočetní techniky.

Na další část textu se podívejte až po malé přestávce, kterou si právem zasloužíte.

2 Struktura sítě WLAN

Cíle

Po prostudování této kapitoly byste měli být schopni:

- charakterizovat jednotlivé komponenty bezdrátové sítě,
- rozeznávat jednotlivé typy bezdrátových sítí,
- popsat fyzickou vrstvu bezdrátové sítě,
- popsat linkovou (MAC) vrstvu bezdrátové sítě,
- obecně charakterizovat architekturu bezdrátových sítí.

Průvodce studiem

V předchozí kapitole jsme Vám vysvětlili základní pojmy používané v souvislosti s bezdrátovými sítěmi. Doufáme, že Vám tyto informace usnadní nejen další studium, ale využijete je i ve svém pracovním životě. Abyste se mohli v problematice bezdrátových sítí lépe orientovat, seznámíme Vás postupně se strukturou těchto sítí. Tak jako při stavbě domu, kde se také začíná základy, i tady budeme muset začít pěkně od začátku – popisem jednotlivých vrstev architektury bezdrátové sítě.
Uvidíte, že se jedná o velmi zajímavé informace, které Vás budou jistě zajímat!
Stejně jako u předešlé kapitoly i v této kapitole Vás budeme „zatěžovat" trochou teorie. Kapitola je ale poměrně krátká. Navíc nemusíte mít strach, neboť již nepůjde o „suchopárné" informace, ale o konkrétní údaje, které jsou nutné pro pochopení složitosti a rozmanitosti bezdrátových sítí.

Potřebný čas pro studium kapitoly:

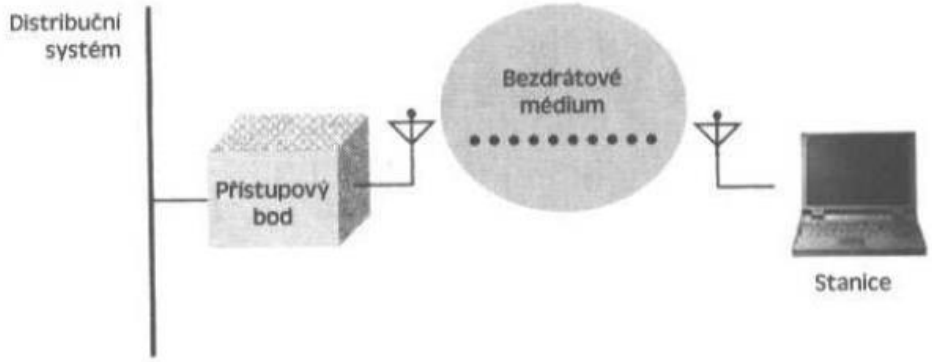
- 60 minut

2.1 Komponenty sítě WLAN

Komponenty IEEE 802.11

Každá 802.11 síť obsahuje čtyři hlavní druhy fyzických komponent:

- Distribuční systém
- Přístupový bod (Access point)
- Bezdrátové médium
- Stanice



Distribuční systém – v okamžiku, kdy má více přístupových bodů tvořit rozsáhlejší síť, musí spolu komunikovat a předávat si informace o pohybu mobilních stanic. Distribuční systém je logická komponenta standardu 802.11 používaná k přesměrování datového toku na stanici skutečného určení podle její aktuální polohy v síti. Ovšem standard 802.11 zatím nespecifikuje žádnou konkrétní technologii distribučního systému, takže komerční produkty řeší tento problém po svém a většinou není možné je při stavbě sítě, kombinovat, pokud je zde požadavek mobility za provozu. V naprosté většině komerčních systémů je distribuční systém řešen jako kombinace síťového mostu (bridge) a distribučního média, jimž je páteřní síť používána pro přenášení dat mezi přístupovými body. Téměř vždy je touto páteřní sítí Ethernet.

Distribuční systém IEEE 802.11

Přístupový bod (Access Point) představuje pravě ono přemostění mezi kabelovou a bezdrátovou sítí, a ačkoliv přístupový bod poskytuje i celou řadu dalších funkcí, funkce mostu mezi bezdrátovou a kabelovou částí sítě je nejdůležitější.

Přístupový bod IEEE 802.11

Bezdrátové médium je pro sítě WLAN tímtéž, co kabeláž pro sítě kabelové – bezdrátové médium je nosičem dat při přesunu dat od stanice ke stanici. Mohli bychom říci, ze tím médiem je vzduch, což je ovšem nesmysl (ostatně sítě WLAN funguji i ve vzduchoprázdnu). Bezdrátovým médiem rozumí 802.11 dvě radiové frekvence (2,4 a 5 GHz) a málo využívanou infračervenou fyzickou vrstvu.

Bezdrátové médium IEEE 802.11

Stanice – bezdrátové sítě se staví proto, aby bylo možné přenášet data mezi jednotlivými stanicemi. Stanici může být obecně jakékoliv zařízení: počítač, notebook, PDA. Nikde není řečeno, že stanice v bezdrátové síti musí byt mobilní a je mnoho sítí WLAN, které propojují počítače prakticky nepřenášené z místa například z důvodu nemožnosti instalace kabelového Ethernetu, z důvodu vytvoření dočasných sítí apod. V takových sítích pak odpadají některé problémy, kupříkladu se nemusí řešit problém mobility jednotlivých stanic.

Stanice

Čtyři výše uvedené komponenty se v praxi shrnuji do dvou nebo tří, protože bezdrátové médium je funkcionalitou využívanou stanicí i přístupovým bodem a distribuční systém.

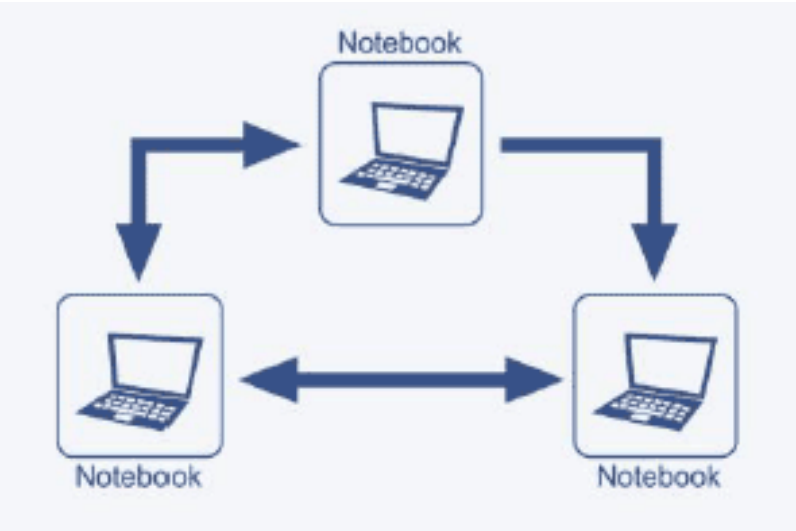
2.2 Typy bezdrátových sítí

Před tím, než začneme stavět či provozovat bezdrátovou síť, je třeba si udělat jasno v tom, jaká bude její základní struktura, tedy jak vlastně chcete mezi sebou propojovat počítače.

Sítě Ad-hoc

Sítě Ad-hoc

Pokud počítačů máte málo, bude asi nejjednodušší metodou spojit tyto počítače mezi sebou sítí na bázi peer-to-peer, kdy všechny počítače jsou si rovnocenné. Tak se to běžně dělá v případě kabelových sítí, u sítí bezdrátových je obdobou peer-to-peer propojení nazývána ad-hoc – tedy síť sestavovaná podle potřeby.



Ad-hoc sítě umožňují rychlou, jednoduchou a cenově příznivou výstavbu, mají ale také své stinné stránky. Tou je především fakt, že sítě ad-hoc vyžadují, aby všechny počítače, které spolu mají komunikovat, byly ve vzájemném dosahu, tedy každý musí být v radiovém dosahu s každým počítačem. To nevadí u malého bytu, ale u větších prostorů to často není možné. Sítě ad-hoc se tedy považují za opravdu sítě sestavené jednoduše a rychle v případě potřeby, když například potřebujete data přenést z jednoho notebooku na druhý, pro praktické a trvalé síťování se téměř nepoužívají. Už v okamžiku, kdy dva počítače mají sdílet připojení na internet, a chceme, aby oba počítače byly na sobě nezávislé při připojování na internet, bude lepší takovou síť vytvořit pomoci WiFi home routeru, zařízení integrujícího Access point a „sdíleč internetu" – tedy směrovač dat z vnitřní „sítě" do internetu.

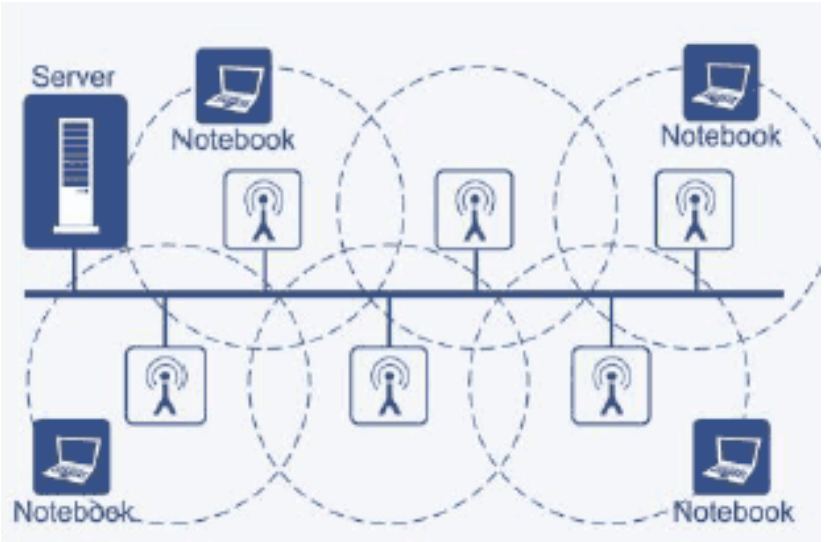
Díky všem těmto omezením a hlavně díky jednoduchosti ad-hoc sítí je již nadále nebudeme uvažovat. Poslední poznámkou k nim budiž fakt, že schopnost práce v ad-hoc sítích musí být na většině zařízení aktivována v menu a protože se zařízení většinou připojují do sítí infrastrukturních a karta musí být zapnuta jen v jednom režimu, výrobci většinou nastavují infrastrukturní režim.

Infrastrukturní sítě

Infrastrukturní sítě

Protipólem sítí ad-hoc jsou sítě infrastrukturní, tedy sítě vybavené speciálním komunikačním prvkem zvaným Access point, zkráceně AP, nebo česky „APéčko". Díky tomu si jednotlivé počítače nemusí povídat přímo mezi sebou, ale komunikují s AP a ten předává jejich komunikaci dále. Každé stanici tedy stačí, aby měla ve svém dosahu alespoň jeden Access point.

Následující obrázek znázorňuje již složitější síť, kde jak vidíte "páteř" tvoří pevně vedený Ethernet, ten propojuje jednotlivé Access pointy a teprve z nich se šíří signál WiFi sítě k notebookům. Aby to bylo veselejší, do této sítě bychom mohli zahrnout roaming, tedy možnost plynulého přechodu z jednoho Access pointu k druhému bez nutnosti změny nastavení sítě.



Na obrázku vidíte příklad takové sítě, kde notebooky jsou do Ethernetu a k firemnímu serveru připojeny právě pomocí bezdrátové sítě.
Přístupový bod je schopen komunikovat s více než jednou stanicí, a proto může propojovat i bezdrátové stanice, které se nalézají v jeho dosahu nezávisle na tom, zda tyto stanice chtějí používat most do kabelového Ethernetu.

Pokud tedy chce jedna bezdrátová stanice komunikovat s jinou stanicí v infrastrukturní síti, musí data putovat dvěma skoky – nejdříve na přístupový bod a z něj teprve na druhou stanici.

V infrastrukturní síti tedy může fungovat každá stanice, která je schopna komunikovat s přístupovým bodem a je v oblasti jeho pokrytí. Ačkoliv se tedy zdá, že infrastrukturní síť má větší nároky na spojovací kapacitu, musíme si uvědomit, že ad-hoc komunikace představuje větší nároky na klientskou stanici, která musí udržovat spojení s každou stanicí, s níž pravě komunikuje.
V infrastrukturní síti stačí udržovat jedno spojeni, a navíc přístupový bod rozpozná, zda stanice přešla do úsporného režimu a může pro ni ukládat data a vyslat je, až se z úsporného režimu probudí. To samozřejmě šetří baterie.

Sekundárních efektů, kvůli nimž použití infrastrukturních sítí převažuje, je samozřejmě více. Infrastrukturní síť nabízí centrální správu, pro uživatele málo orientované v „síťařině" je její nastavení významně jednodušší.

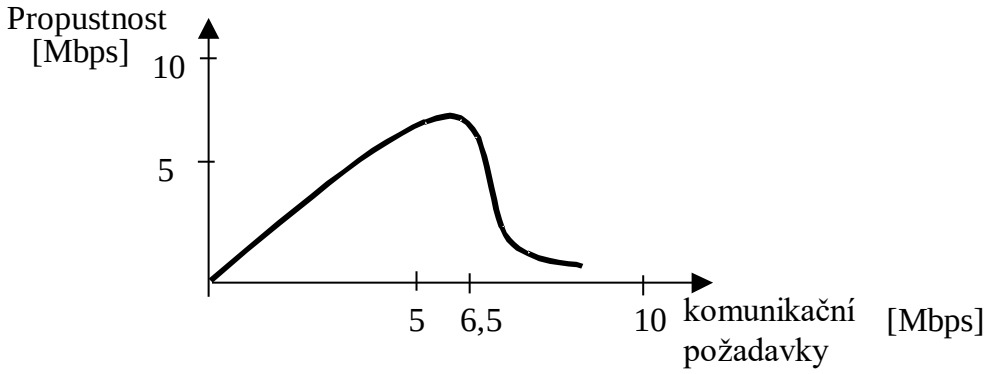
Úkol číslo 3

Které dva typy bezdrátových sítí rozeznáváme?

Pro zájemce

Jelikož jsme se v předchozím výkladu několikrát setkali s pojmem Ethernet, pokusím se vám v této pasáži vysvětlit základy této technologie. Tato lokální síť vychází z počítačové sítě, kterou vyvinula firmou XEROX na začátku 70. let. V současné době se jedná o nejznámější a nejvíce rozšířenou síť. Využívá topologii sběrnice, přenosové médium je zpravidla tvořeno koaxiálním kabelem, ale využívá se i kroucená dvojlinka a světlovodné kabely. Počítačová síť používá přístupovou metodu CSMA/CD a pracuje s teoretickou přenosovou rychlostí 10 Mbps. Vzhledem k použité přístupové metodě je

skutečná přenosová rychlost dána okamžitým zatížením sítě a její maximum je cca 6,5 Mbps. S dalším zatížením v důsledku přibývajících kolizí přenosová rychlost klesá.



Propustnost Ethernetu

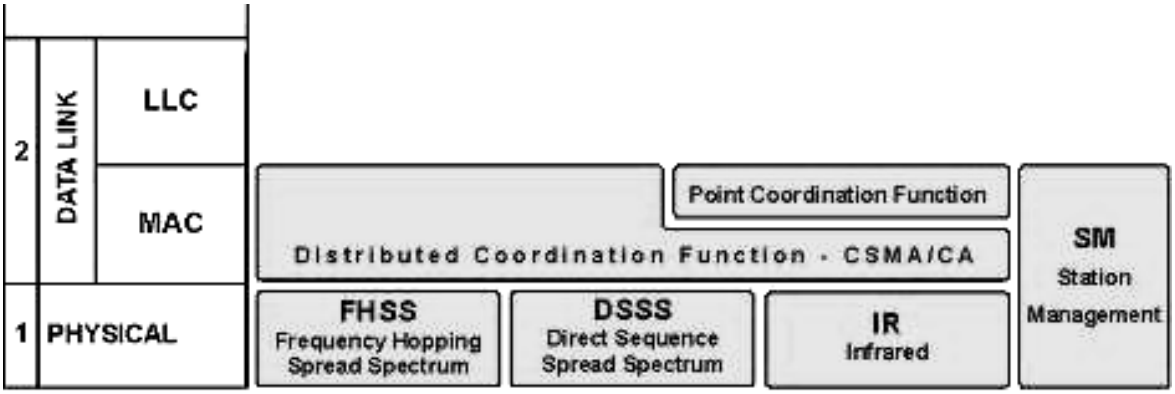
Souhrn všech komunikujících zařízení, které se účastní soupeření o přístup k propojovacímu médiu, se nazývá kolizní doména. Přitom množství přenesených dat připadající na jedno komunikující zařízení s přibývajícím počtem těchto zařízení klesá a nazývá se propustnost.

Propustnost lze orientačně stanovit ze vztahu:

$$p = \frac{\sigma}{2\,N} \qquad [\mathrm{MHz}] \qquad \text{kde}: \sigma = 6{,}5\ \mathrm{MHz}$$

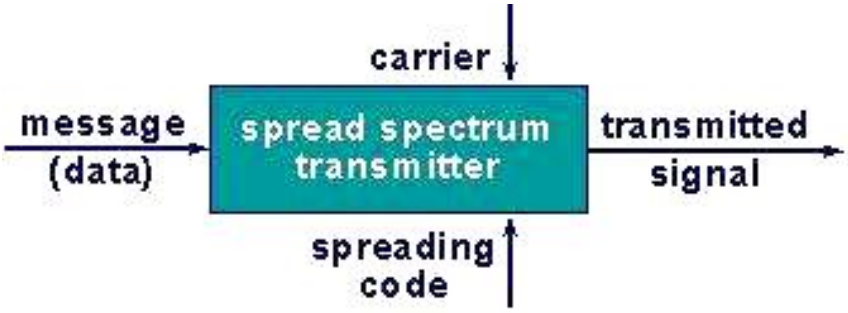
2.3 Fyzická vrstva bezdrátové sítě 802.11

Jako všechny standardy řady 802.x zahrnuje popis první a druhé vrstvy OSI modelu, přesněji řečeno fyzické a MAC vrstvy (viz. obr.).



Pro fyzickou vrstvu je definován přenos pomocí infračerveného světla a rádiový přenos v rozprostřeném spektru a to technikou přímé sekvence (DSSS, Direct Sequence Spread Spectrum) nebo technikou přeskoku kmitočtů (FHSS, Frequency Hopping Spread Spectrum). Systémy pracující infračerveným přenosem pracující v pásmu 850 – 950 nm jsou schopny pokrýt prakticky jen jednu místnost, protože pevné překážky infračervené světlo nepropouští, a z tohoto důvodu nejsou příliš zajímavé. DSSS a FHSS

Co si představit pod pojmem rozprostřené spektrum? Šířka pásma vysílaného signálu je mnohem větší než šířka pásma originálního přenášeného datového signálu – zprávy. Vysílaný signál je určen datovou zprávou a rozprostírací funkcí (kódovou sekvencí, Spreading code; viz. obr.), nezávislou na datové zprávě a známou jen vysílači a určenému přijímači.



Co to znamená v praxi? Tyto systémy jsou imunní vůči interferencím generovaným jinými signály, ať toho už rozprostřenými nebo úzkopásmovými, přítomnými ve stejném frekvenčním pásmu. Také jsou obtížně zachytitelné.

Bezlicenční pásmo 2,4 GHz

V důsledku mohou být systémy s rozprostřeným spektrem umístěny v jednom místě bez nutnosti koordinace, jinými slovy bez přidělování frekvencí. Výsledkem toho je, že jejich provoz není zpoplatňován. Pro bezlicenční provoz je nejen u nás vyhrazeno pásmo 2,4 – 2,4385 GHz. Z technického pohledu používají tyto systémy dva modulační procesy:

- modulace prováděná kódovou sekvencí (Spreading Code)
- modulace prováděná datovou zprávou.

U DSSS jsou jednotlivé bity přenášeny pomocí jedenácti tzv. chipů. Důsledkem toho je, že zpráva je přenášena v širším frekvenčním spektru, každý datový bit je reprezentován známou sekvencí a ne všechny chipy jsou tudíž potřebné pro správnou demodulaci. Použití odlišných sekvenčních kódů pak umožňuje umístění více DSSS systémů v jednom místě.

U FHSS je jako sekvenční kód použita sekvence až 78 možných frekvencí. Datová zpráva je tak vysílána pomocí mnoha nosných frekvencí tzv. hops. Vysoké spolehlivosti je dosaženo díky tomu, že nepotvrzené tj. chybně přenesené rámce jsou znovu přenášeny s jinou nosnou frekvencí tj. v dalším hopu. Umístění více systémů v jednom místě je umožněno použitím různých sekvencí v každém systému.

Standard podporuje rychlosti 1 a 2 Mbps pro oba systémy. Nový standard 802.11b definuje rychlost 11; 5,5; 2 a 1Mbps, ale pouze pro systémy pracující DSSS technikou.

Oba systémy mají své výhody a nevýhody:

- FHSS umožňuje koexistenci více systémů (System Collocation) v jedné lokalitě. Teoreticky až 26, prakticky cca 15.
- U DSSS jsou to pouze 3 systémy bez vzájemného rušení. Je to dáno tím, že pro koexistenci více systémů by byl nutný větší počet chipů, např. pro 16 systému by to bylo 255 chipů. To by znamenalo požadavek na mnohonásobně rychlejší rádiový přenos než je prakticky nemožné.
- DSSS systém má větší propustnost. FHSS spotřebovává část času na přeskok a synchronizaci na jinou frekvenci.
- FHSS má menší problémy s vícecestným šířením signálů. DSSS pracuje s vyšší modulační frekvencí, tím pádem s kratšími symboly a je tak více citlivý na různá zpoždění přijímaných signálů.
- DSSS systém je schopný si poradit s vyšší úrovní interferencí. Při silném rušení, které blokuje některé frekvence, je naopak FHSS systém schopný fungovat na nerušených frekvencích. Totéž platí pro tzv. near/far problém, kdy blízký zdroj interferencí může způsobit zablokování přijímače. FHSS systém může dále fungovat na neblokovaných frekvencích.
- DSSS používá pro příjem a vysílaní různá oddělená pásma, může tak i v plném duplexu používat pouze jednu anténu s filtrem na vstupu přijímače.

Pokud jde o složitost rádiové části a tím de facto i ceny, platí trochu zjednodušeně, že implementace FSK (Frequency Shift Key) pro FHSS je jednodušší než PSK (Phase Shift Key) používané DSSS systémy.

Pro zájemce

Fyzická vrstva v jakékoliv bezdrátové síti definuje modulační a signalizační charakteristiky přenosu dat. Na fyzické vrstvě jsou definovány tři způsoby přenosu dat: dva rádiové a jeden infračervený.

Provozování bezdrátových LAN v nelicencovaných pásmech požaduje modulaci s rozprostřeným spektrem, které jsou v 802.11 definovány dvě (1, str. 300):

- FHSS (Frequency Hopping Spread Spectrum)
- DSSS (Direct Sequence Spread Spectrum)

Obě tyto architektury pracují na frekvenci 2,4 GHz s šířkou pásma 83 MHz (tedy od 2,400 GHz do 2,483 GHz). Jako modulační metodu používá FHSS dvou až čtyřúrovňovou modulaci GFSK (Gaussien Frequency Shift Keying), DSSS pak diferenční BPSK a DQPSK.

2.4 Linková (MAC) vrstva bezdrátové sítě 802.11

Jak je vidět na výše uvedeném obrázku, standard 802.11 definuje dvě přístupové metody – DCF (Distributed Coordination Function) a PCF (Point Cordination Function). PCF je pouze volitelný mechanismus, který slouží pro přenos aplikací citlivých z hlediska času, například hlasu a videa. DCF

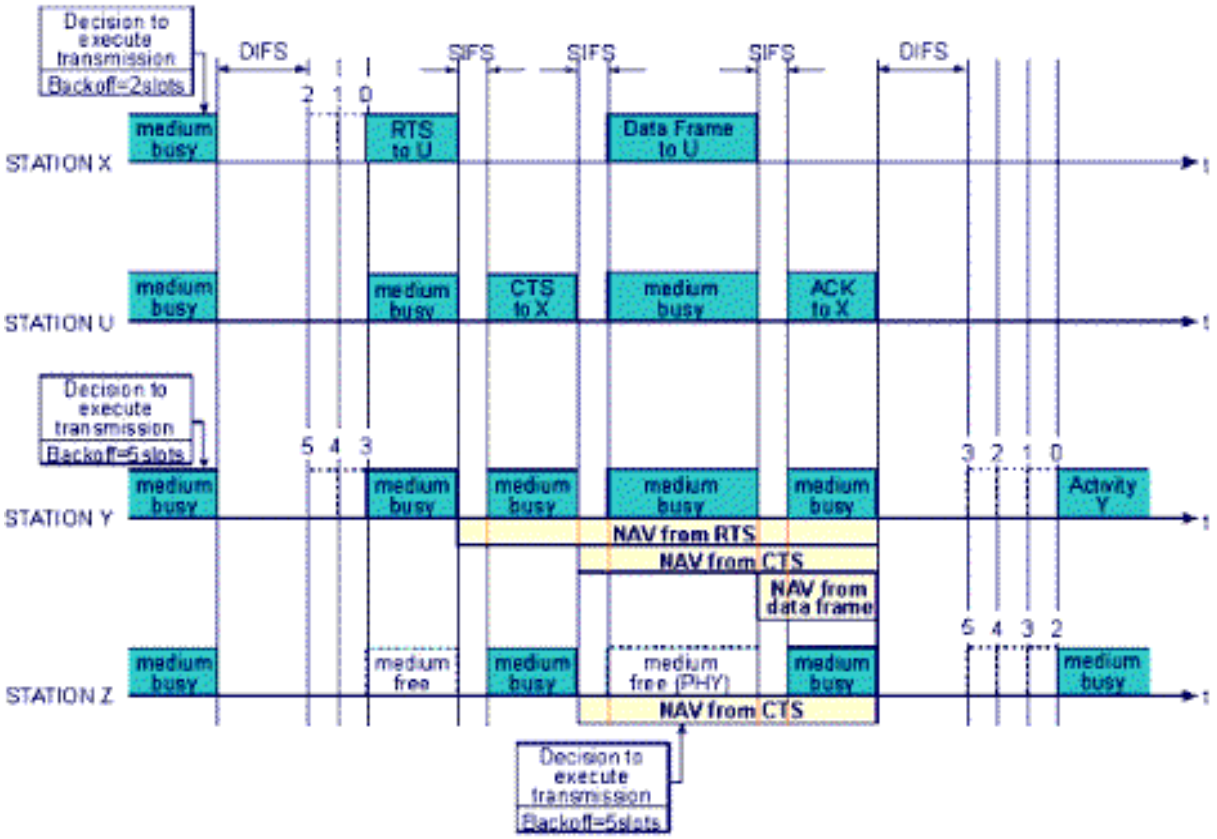
Základním přístupovým mechanismem neboli distribuční koordinační funkcí je CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance). CSMA/CA

CSMA je mechanismus použitý u klasického Ethernetu. CS (Carrier Sense) znamená, že stanice před vysíláním naslouchá na médiu a začne vysílat pouze, pokud je médium volné. MA (Multiple Access) znamená, že je umožněn současný přístup více stanic k médiu. Rozdíl je v tom, že klasický Ethernet používá mechanismus detekce kolizí (Carrier Detection). U bezdrátového Ethernetu je použit mechanismus předcházení kolizí (Collision Avoidance). Proč?

U klasického Ethernetu, např. na koaxu, může každá stanice slyšet vysílání jiné stanice a detekovat kolizi. Tento základní předpoklad pro detekování kolizí u bezdrátového Ethernetu neplatí. Stanice může detekovat volné médium ve svém okolí, to však neznamená, že je volné i u přijímače. Jak je uvedeno výše, stanice komunikují prostřednictví AP a nemusí se tak vůbec přímo slyšet s jinou stanicí ani detekovat její vysílání. Proto je použit mechanismus předcházení kolizím spolu s kladným potvrzováním. To znamená, že stanice naslouchá a pokud je médium volné počká ještě určený čas (DIFS, Distributed Inter Frame Space) a teprve pak začne vysílat. Přijímající stanice zkontroluje kontrolní součet (CRC) přijatého paketu a odešle potvrzení (ACK). Přijetí potvrzujícího paketu znamená pro odesílající stanici, že nedošlo ke kolizi. Pokud stanice ACK paket nedostane, opakuje vysílání. Ethernet

Pro snížení pravděpodobnosti kolizí způsobených tím, že se stanice nemohou slyšet, definuje standard "virtuální" naslouchací mechanismus. Stanice, která chce vysílat, pošle nejdříve krátký řídící paket (RTS, Request To Send), který obsahuje kromě zdroje a cíle i trvání následujícího přenosu. Cílová stanice odpoví jiným řídícím paketem (CTS, Clear To Send), který rovněž obsahuje dobu trvání následujícího přenosu. Stanice slyšící RTS a/nebo CTS paket si nastaví indikátor virtuálního naslouchání, tzv. NAV (Network Allocation Vector) na dobu trvání přenosu. Jinými slovy bude po tuto

dobu brát médium jako obsazené. Snižuje se tak pravděpodobnost kolize ze strany ostatních stanic v lokalitě příjemce pouze na dobu vysílání RTS, protože pak už zachytí paket CTS a budou brát médium jako obsazené. Takový mechanismus je efektivní pouze pro delší pakety, proto standard umožňuje také přenos bez RTS/CTS mechanismu. Tato možnost je volitelně nastavitelná na stanici (RTS Treshold). Rovněž multicasty a broadcasty se nepotvrzují. Následující diagram nám ukazuje, jak celý proces komunikace probíhá.



Pro zájemce

Ethernet pakety mohou mít délku až 1518 B. V případě bezdrátového přenosu je vhodnější používat spíše kratší pakety. Důvod? V případě větší chybovosti rádiového spoje je pravděpodobnost, že dojde k poškození paketu úměrná jeho délce. Také retransmise menšího paketu např. v důsledku kolize představuje menší zátěž pro síť. Nemělo by samozřejmě smysl zavádět nový protokol, který by neuměl pracovat s takto dlouhými pakety. Byl proto definován mechanismus fragmentace a znovu sestavení paketů na MAC vrstvě. Jedná se o jednoduchý algoritmus "pošli a čekej", kdy vysílající stanice vysílá další fragment teprve na základě potvrzení, nebo opakuje vysílaní nepotvrzeného fragmentu. Po určitém počtu neúspěšných retransmisí daného fragmentu je zahozen celý rámec.

Předtím se však stanice musí připojit do sítě. Jak? Musí se synchronizovat se svým AP. Standard připouští pasivní a aktivní skenování. V prvém případě stanice čeká na speciální synchronizační rámec, tzv. Beacon, který je posílán AP v pravidelných intervalech. Beacon slouží především k synchronizaci, která je kritická zvláště pro systémy FHSS, kdy všechny zúčastněné stanice musí měnit frekvenci neboli "hopovat" v jednom okamžiku. V druhém případě se sama stanice snaží najít AP vysíláním rámce Probe Request, na který AP odpovídá rámcem Probe Response. V okamžiku kdy stanice najde AP následuje ověření, kdy si obě strany vymění heslo. Po úspěšném ověření dojde k samotné asociaci

stanice s AP, během které si stanice s BSS vymění informace o svých vlastnostech a stanice je lokalizována v rámci distribučního systému. Teprve pak je stanici umožněno posílat data. Volitelně může být tato procedura ještě rozšířena o WEP algoritmus popsaný výše.

Jednou z nejzajímavějších vlastností bezdrátových sítí je roaming, tzn. přechod stanice z jedné buňky do druhé bez ztráty spojení. Standard 802.11 nedefinuje, jak by měl roaming probíhat, definuje pouze základní služby pro jeho podporu (aktivní/pasivní skenování, re-asociaci...). Proto se i možnosti roamingu u jednotlivých výrobců liší. Nejdále je v současné době zřejmě firma BreezeCom, podporující roaming až do rychlosti 60 km/h.

Úkol číslo 4

Které dvě přístupové metody definuje standard 802.11?

2.5 Architektura bezdrátové sítě 802.11

Základem je přístupový bod (AP, Access Point). Jedná se vlastně o bezdrátový hub, prostřednictvím kterého probíhá veškerá komunikace vzduchem (WM, Wireless Medium). Jinými slovy bezdrátové stanice (station, STA) spolu nikdy nekomunikují přímo, ale vždy prostřednictvím AP. Výjimku tvoří pouze tzv. ad-hoc bezdrátové sítě, kde přístupový bod není nutný. Access Point

Přístupový bod pokrývá signálem základní oblast služeb (BSA, Basic Service Area), stručně řečeno vytváří buňku. Skupina stanic v jedné buňce, připojených k jednomu AP, vytváří základní soubor služeb (BSS, Basic Service Set). BSA

Oblast pokrytí jedné buňky je samozřejmě geograficky limitována a pro pokrytí větší oblasti je potřeba více buněk. Tyto buňky jsou propojeny prostřednictvím distribučního systému (DS, Distribution System) a dohromady vytvářejí rozšířenou oblast služeb (ESA, Extended Service Area). Stanice v této oblasti pak tvoří rozšířený soubor služeb (ESS, Extended Service Set). Buňky sítě

Buňky se mohou překrývat částečně (např. BSA#3, BSA#4) a umožňují pak roaming, tzn. plynulý přechod mobilní stanice z jedné buňky do druhé bez ztráty spojení, nebo úplně (BSA#5, BSA#6, BSA#7). Pak mohou jednotlivá AP (collocated AP) sdílet zátěž (load sharing).

V jedné oblasti mohou existovat i naprosto nezávislé sítě, aniž by o sobě teoreticky musely vědět. Pro připojení (association) k buňce je nutné znát jedinečný identifikátor (tzv. ESSID), kterým se každá stanice musí "prokázat" během připojování k AP. Pokud více sítí v jedné lokalitě používá jiný identifikátor, pak tyto sítě fungují de facto jako fyzicky oddělené (ESA/ESS #1, ESA/ESS #2).

Mimo připojení (association) k AP patří k základním službám přepojení (re-association) z jednoho AP na druhé během roamingu a odpojení (dis-association) při přechodu z jedné buňky do druhé.

Shrnutí

- Každá 802.11 síť obsahuje čtyři hlavní druhy fyzických komponent: distribuční systém, přístupový bod (Access point), bezdrátové médium a stanice.
- Distribuční systém je logická komponenta standardu 802.11 používaná k přesměrování datového toku na stanici skutečného určení podle její aktuální polohy v síti.

- Přístupový bod (Access Point) představuje pravě ono přemostění mezi kabelovou a bezdrátovou sítí, a ačkoliv přístupový bod poskytuje i celou řadu dalších funkcí.
- Bezdrátové médium je pro sítě WLAN tímtéž, co kabeláž pro sítě kabelové – bezdrátové médium je nosičem dat při přesunu dat od stanice ke stanici.
- Stanice – bezdrátové sítě se staví proto, aby bylo možné přenášet data mezi jednotlivými stanicemi. Stanici může být obecně jakékoliv zařízení: počítač, notebook, PDA.
- Pokud počítačů máte málo, bude asi nejjednodušší metodou spojit tyto počítače mezi sebou sítí na bázi peer-to-peer, kdy všechny počítače jsou si rovnocenné. Tak se to běžně dělá v případě kabelových sítí, u sítí bezdrátových je obdobou peer-to-peer propojení nazývána ad-hoc.
- Ad-hoc sítě umožňují rychlou, jednoduchou a cenově příznivou výstavbu, mají ale také své stinné stránky. Tou je především fakt, že sítě ad-hoc vyžadují, aby všechny počítače, které spolu mají komunikovat, byly ve vzájemném dosahu, tedy každý musí být v radiovém dosahu s každým počítačem.
- Protipólem sítí ad-hoc jsou sítě infrastrukturní, tedy sítě vybavené speciálním komunikačním prvkem zvaným Access point, zkráceně AP, nebo česky „APéčko". Díky tomu si jednotlivé počítače nemusí povídat přímo mezi sebou, ale komunikují s AP a ten předává jejich komunikaci dále. Každé stanici tedy stačí, aby měla ve svém dosahu alespoň jeden Access point.
- Pokud tedy chce jedna bezdrátová stanice komunikovat s jinou stanicí v infrastrukturní síti, musí data putovat dvěma skoky – nejdříve na přístupový bod a z něj teprve na druhou stanici.
- Pro fyzickou vrstvu je definován přenos pomocí infračerveného světla a rádiový přenos v rozprostřeném spektru a to technikou přímé sekvence (DSSS, Direct Sequence Spread Spectrum) nebo technikou přeskoku kmitočtů (FHSS, Frequency Hopping Spread Spectrum).
- Standard 802.11 definuje dvě přístupové metody – DCF (Distributed Coordination Function) a PCF (Point Cordination Function). PCF je pouze volitelný mechanismus, který slouží pro přenos aplikací citlivých z hlediska času, například hlasu a videa.
- Základním přístupovým mechanismem neboli distribuční koordinační funkcí je CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance).
- Základem bezdrátové sítě je přístupový bod (AP, Access Point). Jedná se vlastně o bezdrátový hub, prostřednictvím kterého probíhá veškerá komunikace vzduchem (WM, Wireless Medium). Jinými slovy bezdrátové stanice (station, STA) spolu nikdy nekomunikují přímo, ale vždy prostřednictvím AP. Výjimku tvoří pouze tzv. ad-hoc bezdrátové sítě, kde přístupový bod není nutný.

Kontrolní otázky a úkoly

1. Vysvětlete význam pojmu distribuční systém.
2. Vysvětlete pojem přístupový bod.
3. Charakterizujte pojem bezdrátové médium.
4. Vyjmenujte dva základní typy bezdrátových sítí.
5. Charakterizujte přenos pomocí infračerveného světla a rádiový přenos v rozprostřeném spektru a to technikou přímé sekvence DSSS.
6. Charakterizujte přenos pomocí infračerveného světla a rádiový přenos v rozprostřeném spektru a to technikou přeskoku kmitočtů FHSS.
7. Základním přístupovým mechanismem neboli distribuční koordinační funkcí je?
8. Základem bezdrátové sítě je?

Pojmy k zapamatování

Komponenty sítě WLAN, distribuční systém, bezdrátové médium, přístupový bod, Access point, bezdrátová stanice, síť ad-hoc, infrastrukturní síť, DSSS, FHSS, CSMA/CA, PCF, DCF.

Literatura

Základní:
ZANDL, P. *WiFi – praktický průvodce.* 1. vyd. Brno: Vydavatelství Computer Press, 2003. 217 s. ISBN 80-7226-632-2.
KÖHRE, T. *Stavíme si bezdrátovou síť Wi-fi* [překlad Marek Šiller]. Vyd. 1. vyd, Brno: Vydavatelství Computer Press, 2004. 295 s. ISBN 80-251-0391-9.

Rozšířená (pro hlubší pochopení):
DAVIS, H. *Průvodce úplného začátečníka pro Wi-Fi bezdrátové sítě: není zapotřebí žádných předchozích zkušeností!* [přeložil Karel Voráček]. 1. vyd. Praha: Vydavatelství Grada, 2006. 334 s. ISBN 80-247-421-3.

Průvodce studiem

Tak, teď jste prostudovali jednu z nejobtížnějších kapitol. Gratulujeme! Nejedná se o to, že by snad byla až tak rozsáhlá. Řada uvedených skutečností vám určitě byla známa a nejsou tedy žádnou novinkou. Obtížnost spočívá v tom, že je třeba si uvědomit souvislosti. Ano, souvislosti. A to právě bylo hlavním cílem této kapitoly. Nejen znát jednotlivé názvy zařízení a data jejich vzniku, ale umět si je vybavit i v souvislostech.

Věříme, že i pokud si právě v této chvíli nejste těmito souvislostmi úplně jisti, postačí vám, po krátkém odpočinku a něčem na osvěžení, pročíst si pouze zdůrazněné části textu.

3 Hardware pro WiFi sítě – Access pointy

Cíle

Po prostudování této kapitoly byste měli být schopni:

- obecně charakterizovat zařízení pro bezdrátové sítě WiFi,
- vysvětlit pojem přístupový bod a určit jeho charakteristiku s ohledem na topologii bezdrátové sítě,
- vyjmenovat jednotlivé funkce přístupového bodu a u každé uvést stručnou charakteristiku této vlastnosti a její reálné uplatnění,
- vyjmenovat jednotlivé typy zabezpečení přístupového bodu a bezdrátové sítě,
- charakterizovat systém zabezpečení WEB a MAC filtering,
- popsat jednotlivé provozní režimy přístupového bodu,
- orientovat se v problematice práce přístupového bodu v jednotlivých provozních režimech.

Průvodce studiem

Z předchozí kapitoly již víte, na jakém principu fungují bezdrátové sítě. Nyní již ale opusťme pustou teorii a podívejme se na to, jak dnešní moderní bezdrátové sítě pracují a hlavně z jakých komponent sestávají. V této kapitole se budeme zabývat asi nejdůležitějším hardwarovým prvkem bezdrátové sítě, a tím je přístupový bod, nebo také Access point, či hezky česky „APéčko".

Uvidíte, že se jedná o velmi zajímavé informace, které Vás budou jistě zajímat! Výklad je proložen řadou obrázků tak, abyste si mohli vytvořit co nejreálnější představu o hardware bezdrátových sítí.

Poznatky které načerpáte budou tedy značně konkrétní a opřeny o vytvořené představy, z čehož vyplývá, že studium bude jednodušší. Proto se nenechte zaskočit větším rozsahem, který je ovšem přehledně strukturován.

Potřebný čas pro studium kapitoly:

- 90 minut

3.1 Obecně o zařízeních WiFi sítě

Rozšíření technologie WiFi

Při stavbě WiFi sítě se můžeme setkat se širokým spektrem výrobků všech možných značek i provenience, v poslední době se navíc mohou přidávat WiFi i do výrobků spotřební elektroniky, takže můžete narazit nejenom na běžné počítačové komponenty vybavené podporou WiFi, ale třeba i na HiFi věže a DVD přehrávače s podporou WiFi.

Taková zařízení slibují jednoduché propojení a sblížení světa počítačů a domácích multimédií, díky takovým zařízením si můžete snadno přehrávat své MP3 z věže přes pořádný zesilovač, nebo svůj čerstvě „ripnutý" film přehrát na velké televizi.

Zařízení spotřební elektroniky budou ale mimo náš zřetel. Kromě toho, že se u nás prodávají jen výjimečně, neslouží pro skutečné budováni WiFi sítě a jsou zatím spíše doplňkem a kuriozitou, ač nepopírám, že do budoucna představuje takováto konvergence významný trend.

V dalších částech toto studijního textu se budeme zaobírat problematikou těchto WiFi prvků:

- přístupovými body (Access points),
- anténami,
- konektory.

Úkol číslo 5

Máte doma nějaké WiFi zařízení? Pokud ano, uveďte jaké.

3.2 Access Points (AP)

Přístupový bod obecně

AP komunikuje s bezdrátovými zařízeními ve svém dosahu a stará se o směřování (routování) provozu mezi bezdrátovými klienty a zpravidla také mezi pevnou kabelovou sítí. Teoreticky je samozřejmě možné vyrobit AP pouze na bázi WiFi, který nepracuje vůbec s klasickým Ethernetem, ale protože to v praxi nemá moc smyslu, dělají se vlastně jen Access pointy, které routují provoz nejenom v bezdrátové síti, ale také mají výstup do ethernetu.

Charakteristika přístupových bodů

U Access pointů je důležité dbát na několik důležitých věcí. Především byste měli vědět, že ne každý Access point zvládne velké množství najednou připojených uživatelů. Ty levnější Access pointy si poradí najednou třeba jen s třicítkou uživatelů, ty výkonnější obslouží 60, ale také 254 uživatelů připojených najednou. Více uživatelů se už neřeší kvůli omezenému pokrytí nabízeného jedním WiFi pointem – pokud potřebujete připojit více uživatelů, kupte si více AP, už z dále popsaného důvodu to bude výhodnější.

Sdílení klientů

Tady je ale důležité si uvědomit, že **všichni klienti připojení na jeden AP sdílejí rychlostní pásmo 11 Mbps**, takže stovka najednou připojeních klientů, si musí vystačit s rychlostí 100 Kbps., kterou jim jako jednotlivci může AP přidělit. Už z toho důvodu AP nepodporují více jak 254 klientů.

Duální provoz AP

Některé Access pointy ovšem umožňují „duální provoz". „APéčko" totiž v podstatě není nic jiného, než WiFi PCMCIA karta a trocha přídavného hardware starajícího se o možnost upgrade a management karty, jakož i o routing dat do Ethernetu. Prakticky byste si tedy svůj AP mohli velmi jednoduše udělat z jakékoliv WiFi karty – jenže výrobci vědí, že takových koumáků by se našlo hodně a zatímco ceny WiFi karet jsou cenově velmi nízko tlačeny značnou konkurencí a snadností výroby, Access pointy se prodávají poměrně draho a tak výrobci z normálních WiFi karet se snaží firmware pro fungování v režimu Access point odstranit.

Abychom se dostali k tomu blafáku výrobců: do krabice s Access pointem se přímo dávají PCMCIA karty. Každá taková karta může obsloužit určitý počet uživatelů najednou a hlavně každá ta karta nabízí 11 Mbps. Například Access point Orinoco AP-2000 pracuje se dvěma PCMCIA kartami, které navíc nejsou zahrnuty v jeho ceně. Na jednu stranu je mrzuté, že si je musíte dokoupit, na stranu druhou až se rozhodnete přejít na WiFi5 nebo na rychlejší 802.11g standard, stačí dokoupit nové PCMCIA karty. Takový AP ovšem bývá už docela drahý a hodí se spíše pro potřeby firemních klientů.

Pro zájemce

Proč se Access pointy liší cenou? Je dražší lepší?
Vlastně jsem vám hlavní důvod řekl – některé umožňují pracovat na více kanálech najednou, tedy vlastně umožní násobit pásmo 11 Mbps. Již jsem zmínil fakt, že některá zařízení snesou méně připojených uživatelů najednou, nežli zařízení jiná. Důvod je jednoduchý: procesor, který pohání takový

AP je pomalý a více klientů najednou by nezvládal. Tímto problémem se vyznačují právě levnější „APéčka" určená hlavně pro domácí použití. Problém ale není ani tak v tom, že nemůžete připojit více uživatelů najednou – to u domácích sítí nehrozí, stěží se dostanete přes desítku. Horší je nízká odolnost proti DOS útokům, tedy pokusům o zahlcení takového Access pointu síťovými dotazy – pomalý procesor se s tím zle vyrovnává. Ovšem pokud máte malou domácí síť a nemáte hodně nepřátel (nemusí jít jen o mafii nebo policii, ale stačí blbeček „kámoš" vzdělanější v počítačích), není levný AP špatnou volbou.

WiFi zařízení se ale v principu musí řídit jednotným standardem, takže další odlišnosti jsou spíše v možnostech, které „APéčko" nabízí pro svoji správu, nikoliv v základních funkcích. Základní nastavení jako je specifikace IP adres, nastavení parametrů bezdrátové a drátové sítě, zvládne každý AP, ale můžete toho od svého „APéčka" chtít mnohem více – kupříkladu povolovat či zakazovat přístup uživatelů rozpoznaných podle MAC adresy, limitovat jim vyhrazenou přenosovou kapacitu, „APéčko" může mít i svůj firewall a další vymoženosti. Čím více a čím podrobněji a jednodušeji můžete takové parametry nastavovat, tím vyšší je potenciální cena „APéčka". Asi tedy nepřekvapí, že nejvymakanější software pro správu má Orinoco/Avaya a Cisco, oba také podporují řadu funkcí důležitých pro správce firemních sítí a korporátní uživatele. Také výrobky Nexgear, D-Link, SMC a Linksys jsou velmi slušné a nadupané záležitosti zejména pro menší uživatele, naopak na spodním konci jsou méně známé záležitosti jako Zcomax (Z-Com), iTec, Benq a další podobné výrobky o kterých bych neváhal říci, že jsou „no-name".

Tím ale nelze říci, že takové „no-name" výrobky jsou naprosto nepoužitelné. Právě naopak – technickým fandům se bude líbit, že tyto výrobky zpravidla mají běžnou a standardní sadu funkcí, které nepřekrývají a nerozšiřují firemní vylepšení. Díky tomu uživatel dostává zařízení, které si může při dobré znalosti zásadně upravit a přizpůsobit svým potřebám. I nenáročný uživatel zejména domácího charakteru si s ním vystačí, ačkoliv například management takového iTec zařízení je oproti jen o málo dražšímu D-Linku docela otřesný.

Dnes už je docela běžné, že AP lze upgradovat tak, že si ze stránek výrobce stáhnete soubor s novým firmware a nahrajete jej do svého „APéčka". Tím lze opravit nejrůznější chyby a také někdy doplnit nové funkce, ačkoliv ty si výrobce zpravidla nejraději nechává do nového výrobku. Přesto – u dražších výrobců lze očekávat, že chyby relativně rychle opraví a nabídnou novou verzi, případně že nějakou tu novou funkci doplní. Jisté to ale není.

Některé firmy přicházejí s vlastním rozšířením standardu WiFi směrem k dosud nehotovému 802.11g – a tedy nabízejí rychlosti 22 Mbps (třeba D-Link, USRobotics nebo SMC) – tyto rychlosti jsou ale proprietární a budou fungovat jen v případě, když si koupíte veškerou výbavu téhož výrobce.

3.3 Co všechno další může AP umět

Funkce AP

Samotné připojení domácí sítě k internetu se stává základní vlastností AP (přesněji řečeno AP routeru), a k ní se váže široká škála dalších funkcí, které takové zařízení může nabízet. Pravdou je, že většinu z toho o čem si tu teď budeme povídat, se dá zajistit pomocí staršího počítače nejlépe s Linuxem na palubě. Z mnoha důvodů to ale není pro většinu zájemců ideální řešení. Mezi nevýhody patří nesporně i hlučnost a vysoká spotřeba elektrické energie.

Vzhledem k tomu, že většina dnešních routerů je tak jako tak určitým způsobem postavených na Linuxu a tomu je přizpůsoben i výkon jejich CPU, lze od nich požadovat úkoly dříve zajistitelné právě

jedině pomocí vyhrazeného počítače. A to bezhlučně, s vysokou spolehlivostí a minimálními nároky na prostor.

Překlad adres a zabezpečení privátní sítě

Překlad adres

Hlavním bezpečnostním prvkem většiny levných routerů je vnitřní překlad adres privátní sítě na jednu veřejnou adresu poskytnutou ISP. Tento překlad je po prvním zapojení zkonfigurován jako jednosměrný. Je tedy možné přistupovat z privátní sítě k internetu, ale opačně to nelze.
Pro většinu uživatelů je tato konfigurace naprosto dostatečná a nikdy nezatouží po změně. Je dobré ale zjistit jak široce lze vnitřní překlad adres konfigurovat. K základu by mělo patřit otevření libovolných portů pro provoz směrem do privátní sítě pro TCP a UDP protokol. Pokud chcete mít ve vnitřní síti VPN PPTP server (tedy třeba VPN server na MS Windows XP nebo 2003), tak je pro vás důležité aby váš router uměl do privátní sítě přeložit i libovolný jiný IP protokol (pro PPTP konkrétně IP protokol 47).
V tomto kontextu je hodně diskutovaná i UPNP funkcionalita u routerů. Jde o metodu, pomocí níž si sama aplikace běžící na počítači v privátní síti dokáže otevřít požadovaný port na routeru pro příchozí provoz. Na platformě MS Windows lze pozorovat pomalý nárůst popularity této služby, takže pokud jí váš router bude disponovat, není to od věci.

DHCP server

DHCP server

Automatické přidělování IP adres počítačům v privátní síti je opět základní vlastností téměř všech routerů. Přesto se v implementaci této funkce najdou velké rozdíly. Informujte se, zda vámi vybraný zařízení disponuje tzv. předrezervací. Tedy možností přidělit určité MAC adrese v privátní síti předem vybranou IP adresu. Zamezí se tak změnám IP adres u méně často používaných počítačů v privátní síti.
Druhou zajímavou funkcí je možnost omezit rozsah (pool) IP adres, které router používá pro rozdělování. I tato funkce umožní přidělit některým počítačům v privátní síti statické IP adresy bez rizika, že dojde ke konfliktu s těmi automaticky přidělenými.

Tiskový server

Print server

Dostáváme se k vlastnostem, kterými zdaleka nedisponují všechny routery. Připojení tiskárny k jednomu počítači v síti a z něho ji sdílet není ideální řešení. Takový počítač musí být pak zapnout v každém okamžiku, kdy chcete tisknout. Opět šetříte náklady na elektřinu a nervy. Dávejte pozor, jakým portem (USB nebo LPT) router disponuje. Logicky musí odpovídat tomu, přes nějž se připojuje tiskárna. Samotná přítomnost daného portu na routeru ovšem nestačí. Router musí přímo nabízet funkci sdílení tiskárny. Každopádně je dobré si tuto funkci s vaší tiskárnou vyzkoušet, protože levné GDI tiskárny tento způsob připojení často nepodporují a fungovat nebudou.

Webkamera

Webkamera

Některé routery umožňují přímo k nim připojit USB webkameru a pomocí ní pak monitorovat okolí. Tato funkce má většinou smysl hlavně pro přístup z internetu, takže se ujistěte, zda na www stránku s obrazem z webkamery lze přistoupit i z vnějšího rozhraní. Opět je velice důležité zkontrolovat, zda daná USB webkamera funguje s vaším routerem. V tomto případě je nejlepší nakupovat podle seznamu podporovaných webkamer na stránkách výrobce routeru. K pokročilým funkcím patří možnost odeslat obrázek v JPG generovaný webkamerou na zvolený email, pokud je zaznamenán pohyb. Nedisponuje-li váš router touto funkcí a vy přesto o monitorování webkamerou stojíte, nevěšte hlavu. Cena IP kamer, tedy kamer, které se připojují přímo přes Ethernet a disponují vlastním www serverem, poslední dobou klesá velmi rychle, takže pomocí vhodného nastavení překladu adres zpřístupníte obraz na internetu i z nich bez přímé podpory na routeru.

Sdílení souborů

File server

Mnohé routery dnes umožňují připojení USB disku (buď flashdisku nebo obyčejného v USB rámečku). Soubory z něho pak lze sdílet v privátní síti anebo k nim dokonce přistupovat přes internet. Záleží na tom jakou formou je tato funkce implementována. Přístup přes FTP je většinou nejjednodušší, ale pro stanice s Windows také nepříliš pohodlný. Vhodnější je orientovat se na sdílení tohoto disku přes Sambu (SMB protokol). To je způsob, který pro sdílení souborů používají i Windows samotné. Připravte se ale na případné řešení problémů (třeba s diakritikou ve jménech souborů).
Zaměřte se na to, jak snadno a v jakém rozsahu lze provést nastavení uživatelských práv a zda lze soubory zpřístupnit i přes internet.

Omezení rychlosti klientů

Traffic shapping

Sdílení čehokoliv vede i ke konfliktům. Takže je dobré možnost kapacitu připojení rozdělit podle pravidel a ne způsobem „co si kdo ukousne, je jeho". Možnosti limitovat jednotlivým připojeným klientům rychlost se říká shaping a malá část nových routerů jím už disponuje. Určitě neuděláte chybu, když si jejich možnosti prostudujete. Počítejte ovšem s tím, že tato funkce nejlépe funguje u připojení k internetu, jejichž rychlost nekolísá. CDMA pro to například není dobrým kandidátem. Také vezměte v úvahu, že tato funkce není určena pro tržní nasazení a to proto, že ji není většinou problém nějakým způsobem obejít nebo ošálit. Pro domácí omezení syna neustále stahujícího filmy je ale velmi vhodná.
Některá zařízení umožňují limitovat přímo určité aplikace. Je tedy možné třeba nastavit vyšší rychlost pro prohlížení www stránek než pro stahování dat přes FTP. Věc, která vypadá na první pohled velmi dobře, selhává u největšího žrouta kapacity dnešní doby. Výměnné sítě (P2P) generují provoz, který se velmi špatně odhaluje, a tedy také omezuje.

VPN

VPN tunely

Možná zatoužíte po propojení dvou privátních sítí (třeba doma a ve firmě) mezi sebou nebo budete chtít do vaší sítě přistupovat přes internet i z cest. Pak je vaším cílem zřízení virtuální privátní sítě (VPN). Implementace je velice různorodá, ale obecně jde o to, že tato funkce umožní počítačům nebo celé síti, které jsou sami o sobě připojeny k internetu, aby měli přístup k prostředkům, které jsou jinak dostupné jen v dané domácí síti. Z notebooku připojeného přes wifi v internetové kavárně se tak dostanete na soubory na disku u vás doma. Hledejte zařízení, která disponují možností zakončení (terminace) VPN spojení. Většina dnešních zařízení umí jen VPN propustit (VPN pass-through), což je dostatečné pouze v tom případě, že pro zakončení VPN budete mít v síti další zařízení nebo stále spuštěný počítač.

Wake On LAN

Zapnutí a vypnutí po síti

Tato technologie má úzkou vazbu na předchozí bod. Když budete chtít přistupovat z cest k souborům na disku vašeho počítače doma budete potřebovat aby byl zapnutý. Není zrovna ekonomické nechávat počítač zapnutý stále. Wake on LAN (nebo také etherwake, magic packet apod.) je speciální síťový paket, který umí probudit vypnutý počítač. K tomu je potřeba uvnitř počítače propojit síťovou kartu kablíkem se základní deskou a povolit tuto funkci v BIOSu. Pak už potřebujete jen zařízení, které „probouzecí" paket pro počítač vygeneruje. A je skvělé, když to může být přímo váš router a jde to ovládat přes www.

DNS server

Názvový server

Jako DNS server sítě za routerem je většinou nastaven právě router samotný. Ve většině případů ale funguje pouze jako předávací DNS server. Všechny požadavky na překlady DNS jmen předá DNS

serveru vašeho poskytovatele internetu. Může být praktické mít možnost do tohoto procesu zasáhnout. Pak je možné si pojmenovat počítače a další zařízení ve vaší privátní síti a nemusíte si pamatovat jejich číselní IP adresy. Pomocí jednoduchého triku s přesměrováním na localhost je také možné odstavit reklamní servery, které přidávají reklamní proužky do www stránek.

SNMP monitoring

Net monitoring

Je praktické vidět jak je vytížená linka do internetu. Kdy jsou špičky a kdy nikdo nic nepřenáší. K tomu potřebujete, aby tyto informace uměl router počítači předat. A to je právě úloha SNMP. Pokud tento protokol váš router podporuje, budete moci třeba generovat grafy s přehledem provozu, jak je znáte z nix.cz.

Vzdálený reproduktor

Reproduktor

Chtělo by se říci horká novinka letošního léta, kdyby nešlo pouze o využití starší technologie. Jde o možnost přesměrovat (anebo kopírovat) zvukový výstup vašeho počítače na USB zvukovou kartu připojenou k vašemu routeru. Můžete tedy připojit vaši věž v obývacím pokoji a přes Ethernet ji „krmit" zvukem z počítače v dětském pokoji. Vyžaduje to router s podporou této funkce, kompatibilní USB kartu, aplikaci pro počítač, která s touto funkcí počítá (třeba Windows Media Player) a samozřejmě věž s line-in (zvukovým vstupem). Na první pohled velice zajímavá funkce trpí tím, že není dořešeno ovládání (přeskočení písničky, zastavení hudby) ze vzdálené lokace, kde zvuk zní.

Úkol číslo 6

DHCP server na přístupovém bodu zajišťuje?

3.4 Zabezpečení AP a WLAN

Existuje několik možností, jakým můžete zabezpečit provoz Vaší bezdrátové sítě na straně klienta i přístupového bodu.

SSID

SSID

SSID představuje jméno sítě WLAN a stanice ho musí znát pro přístup k této síti. Ve skutečnosti představuje SSID velmi slabou formu zabezpečení. AP pravidelně vysílá rámec beacon obsahující toto SSID, a tak není problém běžnými nástroji toto SSID zjistit. U některých AP lze vypnout broadcast vysílání SSID (to pak není součástí rámce beacon). Ale i tak je SSID součástí rámce vysílaného stanicí při připojování k přístupovému bodu (Association request frame) a tak jej lze zachytit a použít. Někteří administrátoři navíc nechávají u svých sítí standardní SSID přednastavené výrobcem a tím to neoprávněným uživatelům ještě více ulehčují.

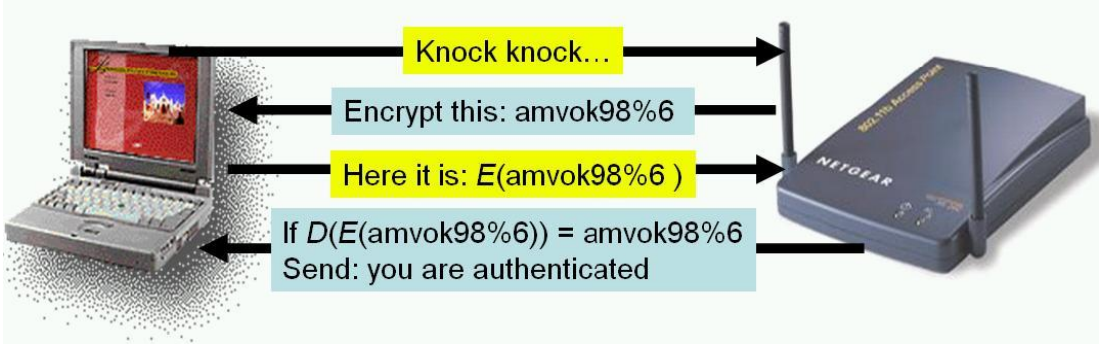
MAC address filtering

MAC

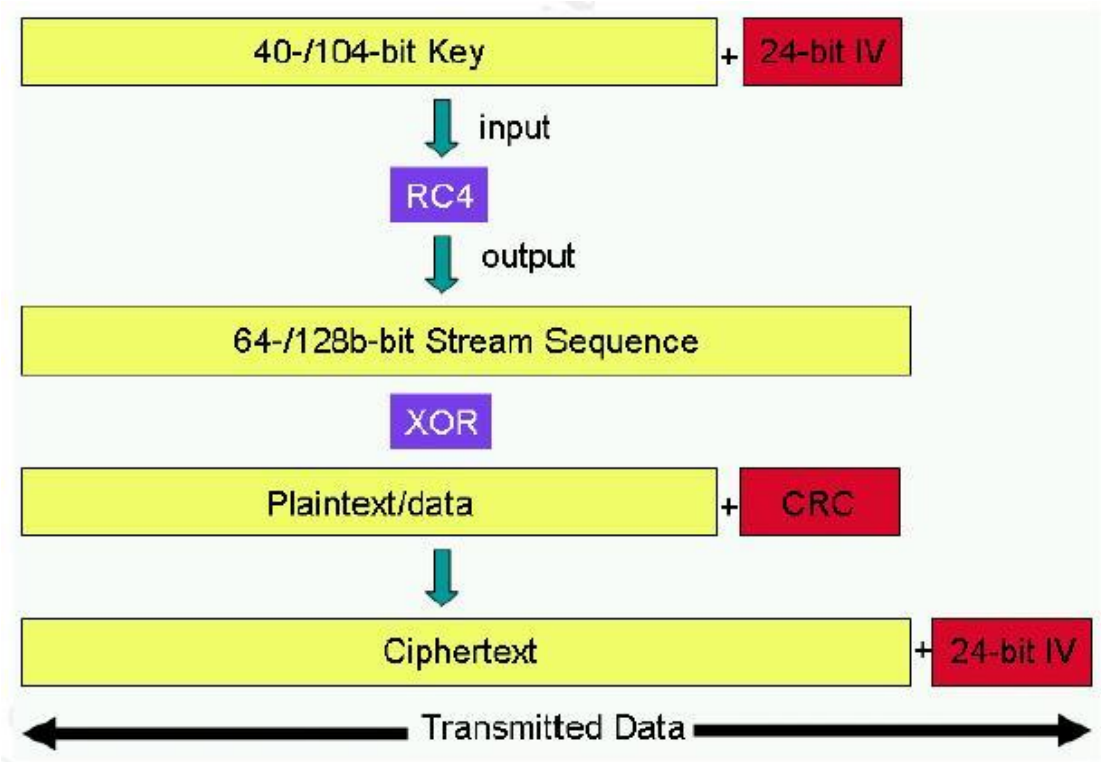
Administrátor WLAN může pro AP vytvořit seznam MAC adres, které s ním mohou komunikovat. Tento přístup je ale značně nepraktický pro sítě větších rozměrů a navíc je neúčinný díky tomu, že lze snadno změnit MAC adresu adaptéru. Odposlechem komunikace lze zjistit některou z platných MAC adres a po přednastavení vlastního adaptéru na tuto adresu se lze po odhlášení původního vlastníka MAC adresy přihlásit do sítě (pokud není použit některý další zabezpečovací mechanizmus).

WEP WEP

WEP (wired equivalent privacy) je volitelný šifrovací standard. Využívá sdíleného klíče (shared key) o délce 40b nebo 104b pro autentikaci uživatelů (resp. NIC adaptérů) a pro šifrování přenášených dat (a jejich CRC).



Proces šifrování dat je na níže uvedeném obrázku.



Nevýhodou WEP je poměrně krátká délka náhodně generovaného inicializačního vektoru IV a díky tomu dochází při častém používání sítě k opakovanému použití stejného vektoru IV. Pokud hacker zachytí dostatečný počet rámců používajících stejný IV (IV je přenášeno v otevřené formě), může toto šifrování snadno prolomit a zjistit sdílený klíč a pak dešifrovat veškerou komunikaci na síti. Standard 802.11 nedefinuje žádné techniky pro změnu sdíleného klíče (tzn., lze ho změnit pouze ručně, což je nepraktické v případě velkého počtu uživatelů) a proto je jeden klíč většinou používán po celou dobu "života" sítě.

WPA WPA

WPA (Wi-Fi Protected Access) je nová bezpečnostní technologie postavená na bázi standardu IEEE 802,11i, která by měla v budoucnu nahradit bezpečnostní techniku WEP, nejrozšířenější v bezdrátovém prostředí. Oproti WEPu nabízí WPA řadu vylepšení, jako je lepší šifrování dat nebo možnost autentizace

uživatele ve větších sítích prostřednictvím různých autentizačních služeb, jako je například RADIUS, ještě před tím, než je do těchto sítí vpuštěn.

802.1x

IEEE 802.1x

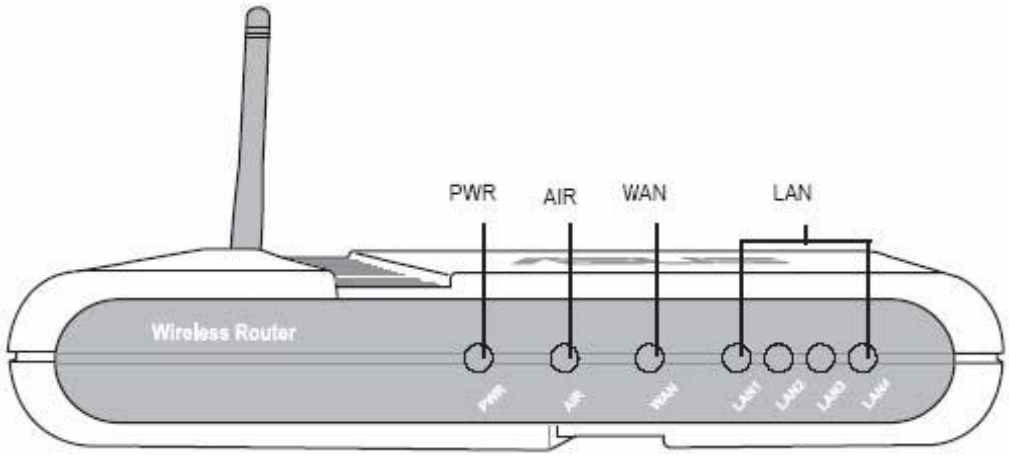
802.1x je obecný bezpečnostní rámec pro všechny typy LAN, zahrnující autentizaci uživatelů, integritu zpráv (šifrováním) a distribuci klíčů. Ověřování se u WLAN realizuje na úrovni portů přístupového bodu WLAN (protokol ale není specifický pro bezdrátové sítě). 802.1x má za cíl blokovat přístup k segmentu lokální sítě pro neoprávněné uživatele. Ověřování ve WLAN provádí přístupový bod pro klienty na základě jejich výzvy pomocí seznamu nebo externího autentizačního systému (serveru Kerberos nebo RADIUS (Remote Authentication Dial In User Service). Pouze ověřený uživatel má možnost přístupu k bezdrátové síti. K šifrování dat v další komunikaci se používají pro každou autentizovanou stanici dynamické klíče. Tyto klíče jsou známy pouze dané stanici, mají omezenou životnost a využívají se k šifrování rámců na daném portu, dokud se stanice neodhlásí nebo neodpojí.

3.5 Režimy provozu AP

Moderní přístupové body dokáží pracovat v několika režimech, které umožňují využití přístupového bodu jako vysílače, klienta či síťového mostu. Možnost nastavení provozního režimu je tedy jednou ze základních funkcí přístupového bodu, kterou je nutné zohlednit při návrhu bezdrátové sítě a nákupu síťových komponent.

Provozní režimy obecně

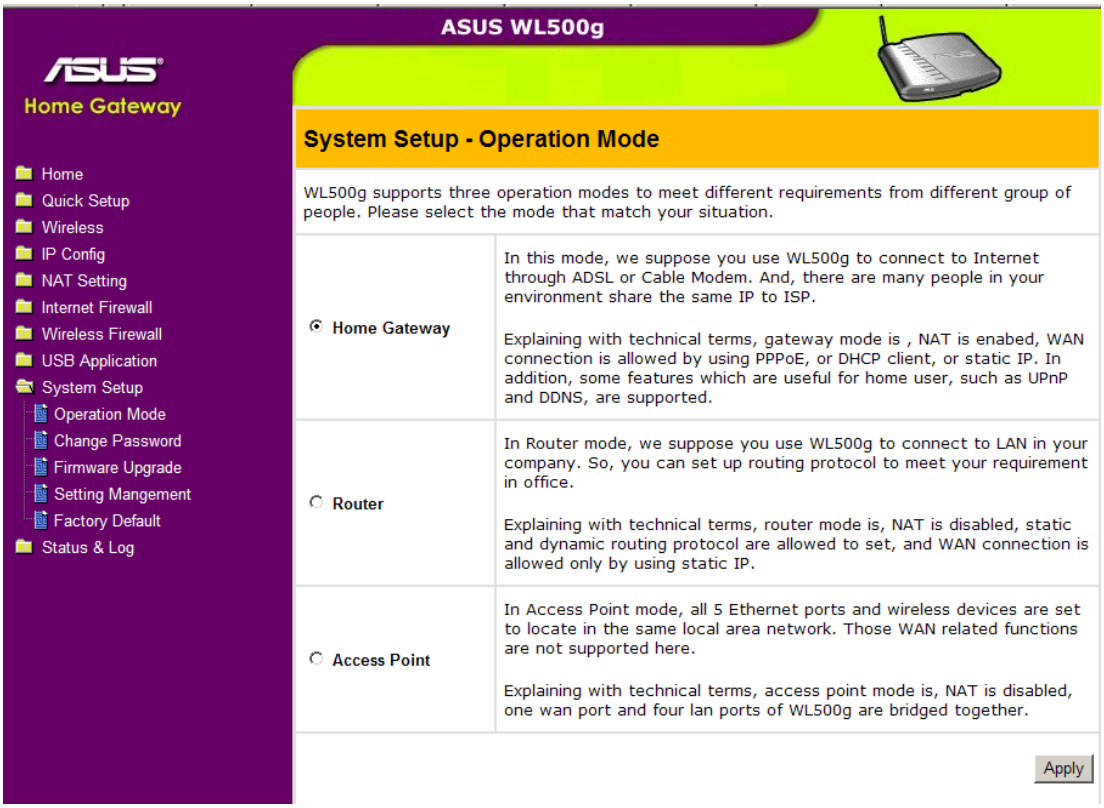
Nastavení, které musíte provést, se tedy bude lišit v závislosti na roli, jakou bude vaše AP v síti zastávat. Jelikož je nastavení provozních režimů u jednotlivých zařízení od různých výrobců takřka totožné, použiji pro další popis jednotlivých režimů velmi oblíbený přístupový bod ASUS WL-500g.



- **PWR** (elektrická síť) – Off: není zapojen do elektřiny, On: systém je připraven.
- **AIR** (bezdrátová síť) – Off: není připojen, On: bezdrátový systém je připraven. Bliká: vysílá nebo přijímá data (bezdrátově)
- **WAN** (vzdálená síť – Internet) – Off: WAN port není připojen, On: WAN port fyzicky připojen do sítě Ethernet. Bliká: vysílá nebo přijímá data (přes síť Ethernet)
- **LAN 1-4** (lokální síť) – Off: příslušný LAN port není připojen, On: port fyzicky připojen do sítě Ethernet. Bliká: vysílá nebo přijímá data (přes síť Ethernet)

Nastavení režimu práce přístupového bodu se provádí pomocí webového konfiguračního rozhraní, jehož obrázek je umístěn níže. Podrobněji se budeme touto problematikou zabývat v dalších částech tohoto výukového materiálu.

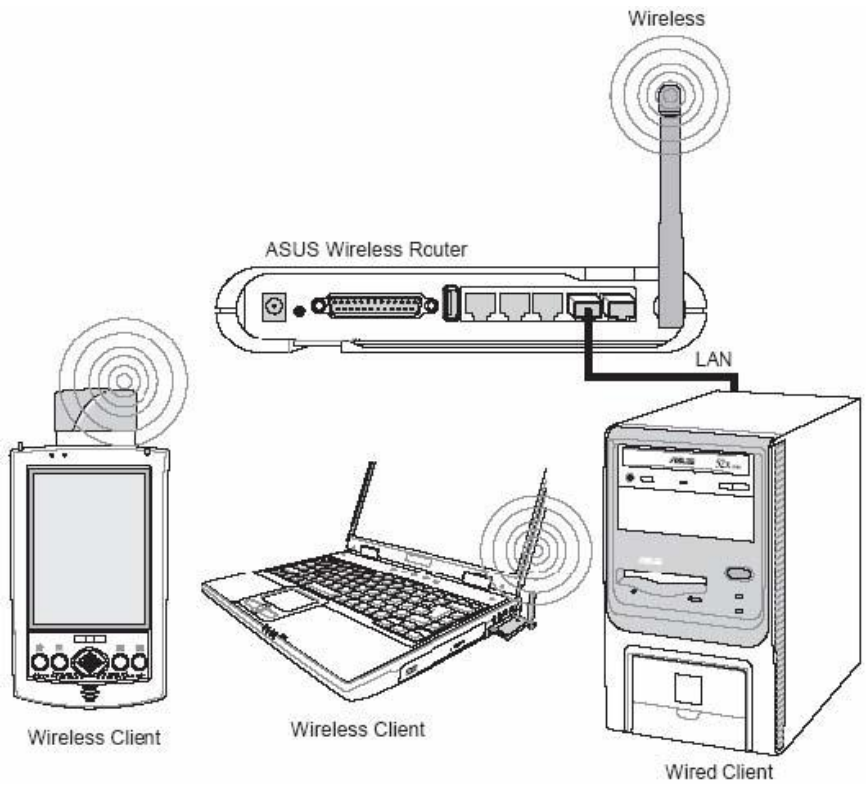
Konfigurační rozhraní



3.5.1 Režim Router

Provozní režim směrovače

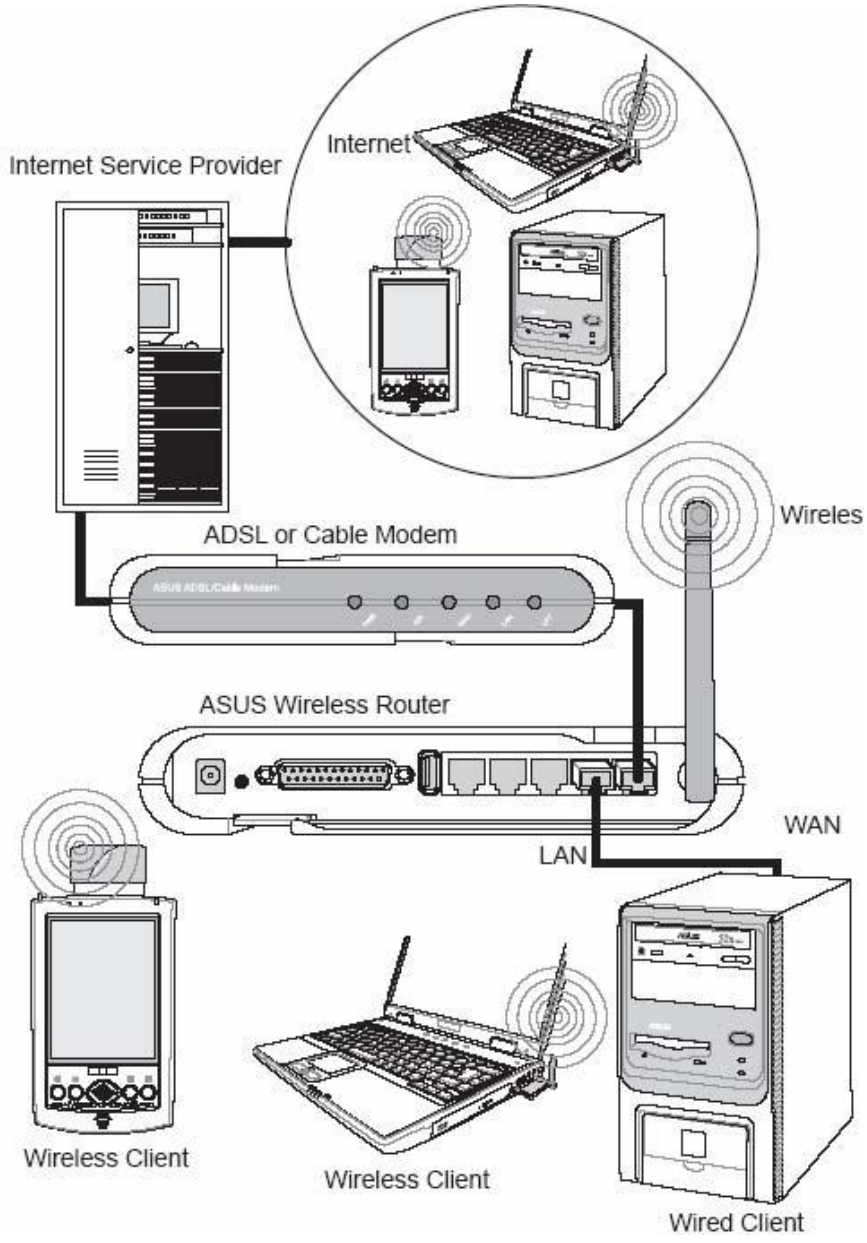
V této topologii spojuje AP dohromady drátová a bezdrátová zařízení a vytváří lokální síť LAN. Pro připojení počítače (či jiného zařízení) do bezdrátového routeru ASUS potřebujete síťový kabel (UTP-Cat5e) jedním koncem zapojený do jednoho z LAN portů na zadní straně bezdrátového routeru ASUS a druhý konec do 10/100 LAN portu u zařízení. Při bezdrátovém připojení musí bezdrátoví mobilní klienti vyhovět normě IEEE 802.11b.



3.5.2 Režim Home Gateway

Provozní režim domácí brány

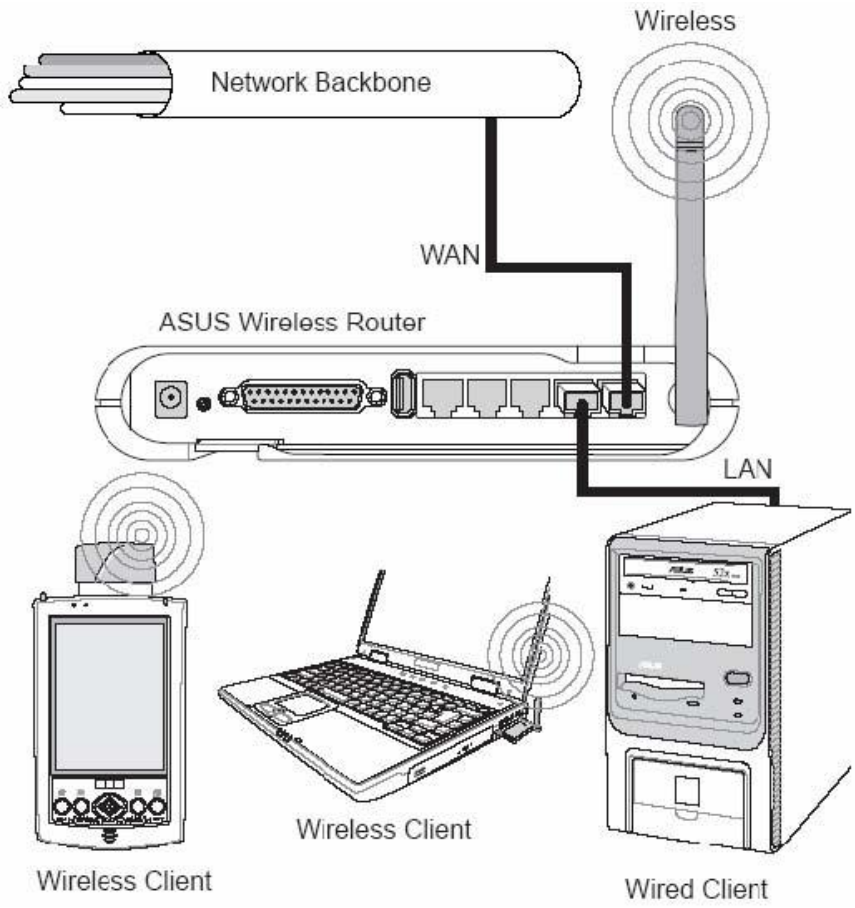
Při této topologii není AP pouze páteří vaší LAN, ale také bránou k vašemu poskytovateli internetových služeb (ISP). Ke komunikaci s vaším ISP můžete použít ADSL nebo kabelový modem. Propojte LAN port na modemu s WAN portem na zadní straně AP ASUS použitím síťového kabelu.



3.5.3 Režim Access Point

V této topologii je AP mostem mezi vaší LAN a jinou sítí. Použijte síťový kabel s jedním koncem zapojeným do WAN portu AP a druhý do jiné sítě tak, jak vidíte na obrázku.

Provozní režim vysílacího bodu



Úkol číslo 7

V kolika režimech (stačí číslo) dokáže pracovat AP ASUS WL-500g?

Shrnutí

- Při stavbě WiFi sítě se můžeme setkat se širokým spektrem výrobků všech možných značek i provenience, v poslední době se navíc mohou přidávat WiFi i do výrobků spotřební elektroniky, takže můžete narazit nejenom na běžné počítačové komponenty vybavené podporou WiFi, ale třeba i na HiFi věže a DVD přehrávače s podporou WiFi.
- AP komunikuje s bezdrátovými zařízeními ve svém dosahu a stará se o směřování (routování) provozu mezi bezdrátovými klienty a zpravidla také mezi pevnou kabelovou sítí.
- U Access pointů je důležité dbát na několik důležitých věcí. Především byste měli vědět, že ne každý Access point zvládne velké množství najednou připojených uživatelů. Ty levnější Access pointy si poradí najednou třeba jen s třicítkou uživatelů, ty výkonnější obslouží 60, ale také 254 uživatelů připojených najednou.
- Je ale důležité si uvědomit, že **všichni klienti připojení na jeden AP sdílejí rychlostní pásmo 11 Mbps**, takže stovka najednou připojeních klientů, si musí vystačit s rychlostí 100 Kbps., kterou jim jako jednotlivci může AP přidělit. Už z toho důvodu AP nepodporují více jak 254 klientů.

- Některé Access pointy ovšem umožňují „duální provoz". „APéčko" totiž v podstatě není nic jiného, než WiFi PCMCIA karta a trocha přídavného hardware starajícího se o možnost upgrade a management karty, jakož i o routing dat do Ethernetu.
- Samotné připojení domácí sítě k internetu se stává základní vlastností AP (přesněji řečeno AP routeru), a k ní se váže široká škála dalších funkcí, které takové zařízení může nabízet. Například jsou to tyto funkce: překlad adres a zabezpečení privátní sítě (NAT), DHCP server, tiskový server (print server), webkamera, sdílení souborů (file server), omezení rychlosti klientů (traffic shapping), VPN (tunelovaná připojení), Wake On LAN (zapnutí a vypnutí přes síť), DNS server, SNMP monitoring a vzdálený reproduktor.
- Existuje několik možností, jakým můžete zabezpečit provoz Vaší bezdrátové sítě na straně klienta i přístupového bodu: SSID, MAC address filtering, WEP, WPA a 802.1x.
- SSID představuje jméno sítě WLAN a stanice ho musí znát pro přístup k této síti. Ve skutečnosti představuje SSID velmi slabou formu zabezpečení.
- Administrátor WLAN může pro AP vytvořit seznam MAC adres, které s ním mohou komunikovat. Tento přístup je ale značně nepraktický pro sítě větších rozměrů a navíc je neúčinný díky tomu, že lze snadno změnit MAC adresu adaptéru.
- WEP (wired equivalent privacy) je volitelný šifrovací standard. Využívá sdíleného klíče (shared key) o délce 40b nebo 104b pro autentizaci uživatelů (resp. NIC adaptérů) a pro šifrování přenášených dat (a jejich CRC).
- WPA (Wi-Fi Protected Access) je nová bezpečnostní technologie postavená na bázi standardu IEEE 802,11i, která by měla v budoucnu nahradit bezpečnostní techniku WEP, nejrozšířenější v bezdrátovém prostředí. Oproti WEPu nabízí WPA řadu vylepšení, jako je lepší šifrování dat nebo možnost autentizace uživatele ve větších sítích.
- 802.1x je obecný bezpečnostní rámec pro všechny typy LAN, zahrnující autentizaci uživatelů, integritu zpráv (šifrováním) a distribuci klíčů. Ověřování se u WLAN realizuje na úrovni portů přístupového bodu WLAN (protokol ale není specifický pro bezdrátové sítě).
- Moderní přístupové body dokáží pracovat v několika režimech, které umožňují využití přístupového bodu jako vysílače, klienta či síťového mostu.
- Nastavení režimu práce přístupového bodu se provádí pomocí webového konfiguračního rozhraní.

Kontrolní otázky a úkoly

1. Co je nejdůležitější částí bezdrátové sítě?
2. V jakých provozních režimech může AP pracovat?
3. Které typy zabezpečení AP a WLAN rozeznáváme?
4. Jaké funkce může AP v bezdrátové síti vykonávat?

Pojmy k zapamatování

Přístupový bod, AP, Access point, WPN, WEB, MAC filtering, WPA, NAT, SSID.

Literatura

Základní:

ZANDL, P. *WiFi – praktický průvodce.* 1. vyd. Brno: Vydavatelství Computer Press, 2003. 217 s. ISBN 80-7226-632-2.

KÖHRE, T. *Stavíme si bezdrátovou síť Wi-fi* [překlad Marek Šiller]. Vyd. 1. vyd, Brno: Vydavatelství Computer Press, 2004. 295 s. ISBN 80-251-0391-9.

Rozšířená (pro hlubší pochopení):

DAVIS, H. *Průvodce úplného začátečníka pro Wi-Fi bezdrátové sítě: není zapotřebí žádných předchozích zkušeností!* [přeložil Karel Voráček]. 1. vyd. Praha: Vydavatelství Grada, 2006. 334 s. ISBN 80-247-421-3.

Průvodce studiem

A opět je zde konec kapitoly. V klidu si udělejte zaslouženou přestávku! Projděte se, rozcvičte se, a nebo si uvařte Váš oblíbený čaj.

Při tom si myšlenkově snažte znovu projít obsah kapitoly. Vůbec nevadí, že si po prvním přečtení nevybavíte řadu pojmů. To je zcela normální. Je ale důležité uvědomovat si, co ještě nevím a co mi dělá potíže. Pak už stačí vrátit se jen k těmto částem! S postupem času zjistíte, že vše perfektně ovládáte.

Pamatujte, chybami se člověk učí! Důležité je ale vědět, v čem dělám chyby. Proto nepodceňujte význam uvedených úkolů a kontrolních otázek.

4 Hardware pro WiFi sítě – Antény

Cíle

Po prostudování této kapitoly byste měli být schopni:

- orientovat se v problematice dosahu bezdrátových sítí,
- analyzovat a vyhodnocovat rušivé vlivy,
- charakterizovat základní typy antén,
- určovat možnosti použití jednotlivých typů antén,
- určovat základní parametry antén bezdrátových sítí.

Průvodce studiem

Jestliže jste zvládli předchozí kapitolu, udělali jste velký kus práce, který je třeba ocenit. Vaší odměnou je velký předpoklad, že zanedlouho úspěšně zakončíte studium této disciplíny. Dosavadní vědomosti by k tomu samozřejmě ještě nestačily, ale budete-li takto pokračovat, úspěch se jistě dostaví.

Udělejme tedy další krok a přejděme od přístupových bodů k dalšímu článku – anténám. Antény jsou nedílnou součástí bezdrátové sítě, protože v ideálním případě pouze na nich závisí, jaký dosah bude mít bezdrátová síť.

Doporučení pro zájemce o hlubší studium:

- zaujala-li Vás hlouběji problematika bezdrátových sítí, můžete si ke kterékoliv kapitole dohledat další informace. Existuje řada internetových stránek, kde jsou podrobně popsány jednotlivé komponenty bezdrátových sítí včetně srovnávacích testů. Můžete tak získat řadu nejaktuálnějších informací.

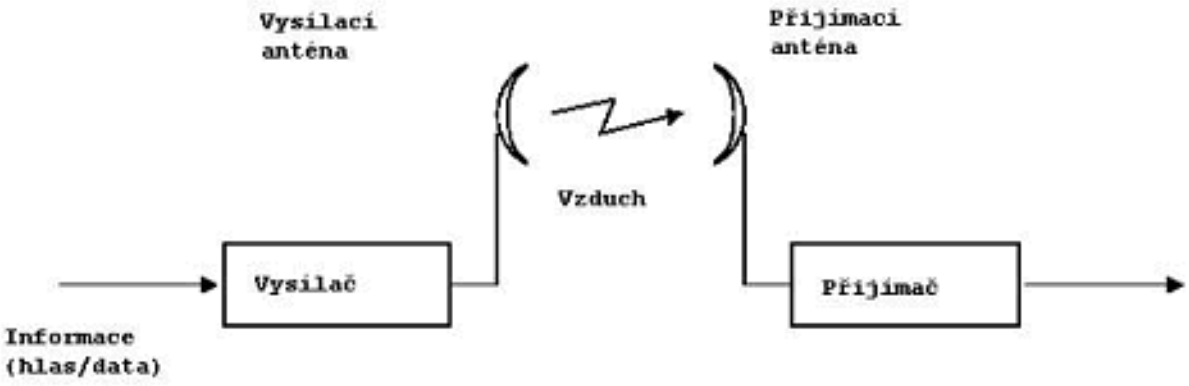
Potřebný čas pro studium kapitoly:

- 45 minut

4.1 Jak daleko "vidí" bezdrátové sítě

První otázka uživatele, který uvažuje o nasazení bezdrátové sítě, je: "Na jakou vzdálenost to vlastně funguje?" A odpověď? Není úplně jednoduchá a může se v závislosti na konkrétních podmínkách výrazně lišit. Nejprve je potřeba ujasnit si některé základní pojmy.

Následující obrázek ukazuje typický rádiový systém. Vysílaná informace jde z vysílače do antény, následně pak v podobě elektromagnetických vln vzduchem do přijímače, kde je informace demodulována do své původní podoby.



Pro libovolný výpočet je nutné znát používané jednotky a definici souvisejících parametrů. Prvním z nich je **výstupní úroveň vysílače** a **vstupní úroveň přijímače**. Hodnota vstupní/výstupní úrovně je vyjádřená ve Wattech případně v dBm, přičemž vztah mezi dBm a Watty může být vyjádřen následovně:

Výstupní a vstupní úroveň vysílače a přijímače

$P_{dBm} = 10 \times \log P_{mw}$.

Příklad: *1 Watt = 1000 mW*, tzn. $P_{dBm} = 10 \times \log(1000) = 30$ *dBm*.

V České republice je maximální výstupní úroveň omezena Generálním povolením ČTÚ č. 01/1994 na 100 mW EIRP, tzn. 20dBm:

$P_{dBm} = 10 \times \log(100) = 20$ *dBm*.

Dalším parametrem je **útlum** znázorněný na následujícím obrázku. P_{in} je hodnota na vstupu, P_{out} je hodnota na výstupu. Útlum se udává v dB a je vyjádřen následujícím vzorcem:

Útlum

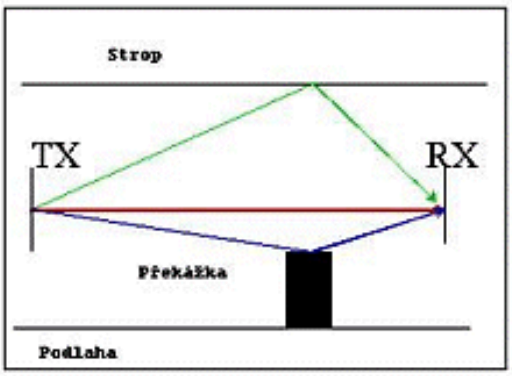
$P_{dB} = 10 \times \log(P_{in}/P_{out})$.

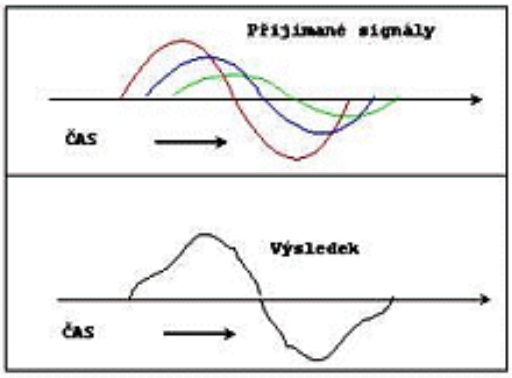
Příklad: Pokud je vstupní úroveň na přijímači poloviční, tzn., že přenosem dojde ke ztrátě poloviny energie $P_{out}/P_{in} = 2$, potom je útlum $10 \times \log(2) = 3$ *dB*.

Útlum závisí na takových parametrech, jako je:

Parametry útlumu

- vícecestné šíření signálu,
- přímá viditelnost,
- počasí, např. vítr, déšť,
- rušení s jinými systémy ve stejném pásmu.





Na tomto místě je však třeba říci, že vliv počasí je minimální. Například i velmi intenzivní déšť 150 mm/h způsobí zeslabení signálu maximálně o 0,02 dB/km. Mnohem významnější jsou pak nepřímé vlivy, jako je např. mokré listí na stromech, které de facto vytváří "vodní stěnu". Voda vlny v pásmu 2,4 GHz nepropouští – mění je na tepelnou energii. Když už jsme u stromů, pokud budete instalaci provádět např. v zimě, pamatujte, že během roku se díky vegetaci mohou podmínky pro šíření rádiových signálů velice radikálně změnit.

4.2 Ztráty na trase a antény bezdrátových sítí

Parametry, které jsme si jmenovaly v předchozí části, způsobují **ztráty na přenosové trase**. Jedná se o ztrátu energie během přenosu rádiového signálu vyjádřenou v dB. Tyto ztráty jsou závislé mimo výše uvedeného na následujících faktorech: Ztráty

- vzdálenost mezi přijímací a vysílací anténou;
- přímá viditelnost mezi příjímací a vysílací anténou;
- vlastní parametry použité antény.

Ztráty při šíření elektromagnetických vln volným prostorem jsou dány následujícím vzorcem:

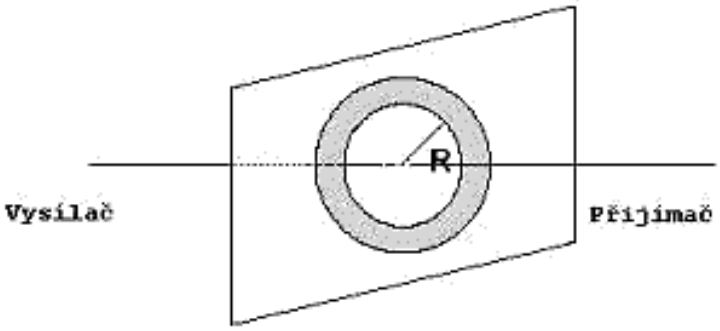
Ztráta_ve_volném_prostoru = 32.4 + 20 x log F(MHz) + 20 x log R(km)

kde F je frekvence v MHz a R je vzdálenost mezi přijímací a vysílací anténou v kilometrech. Protože se jedná o nelicencované pásmo 2,4 GHz, vzorec se nám zjednodušuje na *100 + 20 x log R(km)*.

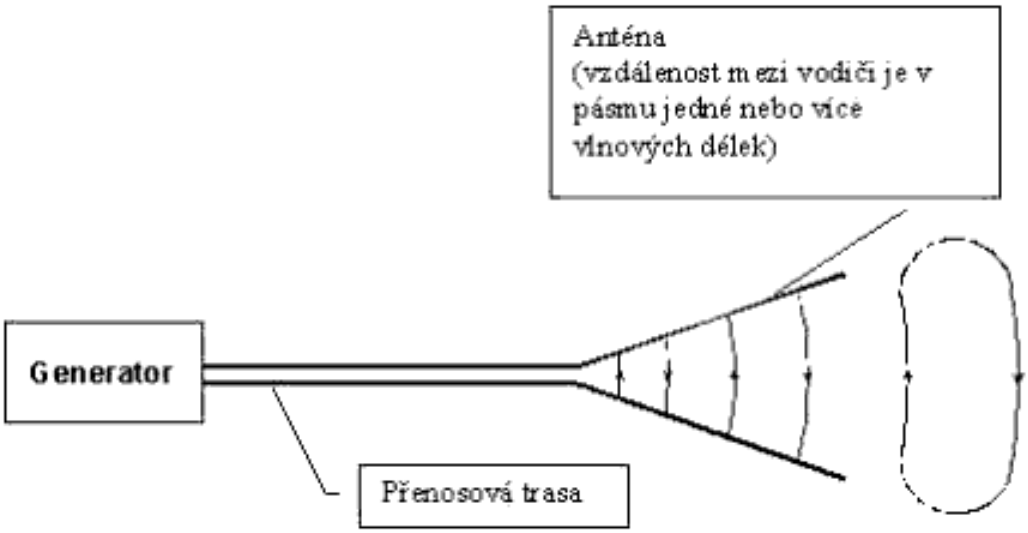
Důležité je si uvědomit, co se myslí pojmem **přímá viditelnost**. Protože se nejedná o laser, nestačí nám optická přímá viditelnost, ale potřebujeme i určitý prostor kolem (viz obr. níže). Jedná se o tzv. **Fresnelovou zónu,** která je definována následovně: Přímá viditelnost

$R_1 = ½ Ö(lxD)$

kde R_1 je poloměr první Fresnelovy zóny, l je vlnová délka a D je délka přenosové trasy. Pokud je 80 % první Fresnelovy zóny volných, potom je šíření signálu stejné jako ve volném prostoru. Jinými slovy, při rádiovém přenosu nám nestačí pouze optická viditelnost, ale mezi případnými překážkami musí být prostor odpovídající aspoň 80 % Fresnelovy zóny. Fresnelova zóna



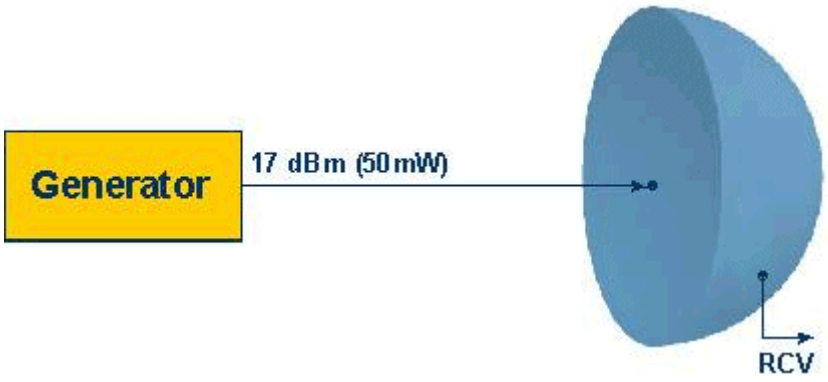
Jedním z nejdůležitějších prvků na kterém závisí kvalita spoje je **anténa**. Anténu zpravidla definujeme jako prvek, který umožňuje přechod elektromagnetického vlnění přiváděného na elektromagnetické vlnění ve volném prostoru (viz obr. níže). Anténa obecně



Jedním ze základních pojmů je **izotropní anténa**. Jde o bod, který rovnoměrně vyzařuje do všech směrů (360°) a to beze ztrát. Jedná se o teoretickou, tj. technicky nerealizovatelnou anténu, která slouží pro výpočty a popis parametrů skutečných antén. Izotropní anténa

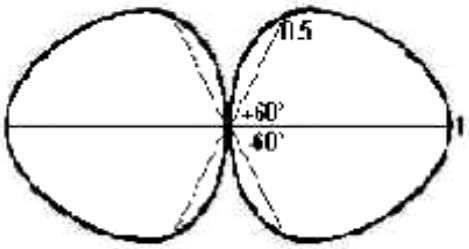
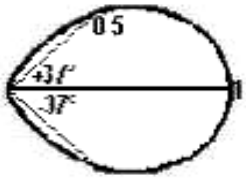
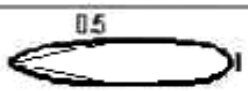
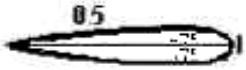
Pomocí izotropní antény se definuje např. **zisk antény**. Jedná se o poměr mezi intenzitou vyzařování v daném směru k intenzitě vyzařování, kterou bychom obdrželi, kdyby energie přijatá anténou byla vyzářena rovnoměrně do všech směrů. Zisk antény se udává v dBi. Zisk antény

Příklad: Anténa ze ziskem 3 dBi vyzařuje do 50 % prostoru (viz obr. níže), tzn. že na přijímači je generována energie 17 dBm. Pokud by stejnou energii měla generovat izotropní anténa, potřebovala by zdroj o výkonu 20 dBm. Rozdíl je tři, což je právě zisk antény. Někdy se uvádí tato hodnota jako ekvivalent energie vyzářené izotropní anténou (EIRP – Equivalent Isotropic Radiated Power). V našem případě by to bylo 20 dBm EIRP.



Z obrázku je zřejmé, že zisk antény úzce souvisí se **směrovostí** a následně pak s dosahem. Tato souvislost je nejlépe patrná při grafickém znázornění **vyzařovací charakteristiky** (viz obr. níže).

Směrovost a vyzařovací charakteristiky antén

Type	Gain (dBi)	Radiation Pattern	HPBW
Omni directional	2		± 60°
Omni directional	6		± 10°
Uni directional	8.5		± 37°
Uni directional	12		±11°
Uni directional	18		± 7°
Uni directional	24		± 3.7°

Útlum kabelu a citlivost přijímače u bezdrátových sítí

Útlum a citlivost

Poslední dva parametry, které potřebujeme znát, jsou **útlum kabelu** a **citlivost přijímače**. Útlum kabelu je dán typem kabelu. Obyčejný RG-58, koaxiální kabel používaný mj. i pro Ehernet, má útlum 1 dB/m. U kabelu RG-214 je to 0,6 dB/m a u speciálního kabelu typu Heliax pouze 0,11 dB/m. Citlivost přijímače je nutné zjistit u výrobce daného zařízení.

Nyní máme dostatek informací, abychom si dokázali odpovědět na naši původní otázku. Na jakou vzdálenost lze tedy použít bezdrátové sítě?

Úroveň přijímaného signálu na vstupu přijímače S_i musí být minimálně rovna citlivosti přijímače, tedy $S_i = P_{out} - C_t + G_t - P_l + G_r - Cr$. P_{out} je výstupní úroveň vysílače, C_t je útlum na anténním kabelu vysílače, G_t jezisk vysílací antény, G_r je zisk přijímací antény, P_l jsou ztráty na přenosové cestě a C_r je útlum na anténním kabelu přijímače. Určitě je rozumné počítat s určitou rezervou např. pro zohlednění vlivu počasí.

Maximální povolený vyzařovaný výkon

Zásadní omezení je dáno Generálním povolením ČTÚ č. 01/1994 které říká, že maximální vyzářený výkon může být 100 mW EIRP. Pro zvětšení dosahu lze použít různé zesilovače, ale vždy pouze v souladu s výše uvedeným povolením.

Na závěr důležité upozornění. Žádný teoretický výpočet nemůže zahrnout všechny případné vlivy jako je rušení apod. Co tedy dělat? Pokud chcete mít opravdu jistotu, nezbývá než vyrazit do terénu a provést reálné měření pomocí zařízení, která budou skutečně instalována. Většina výrobců na tuto možnost pamatuje a nabízí tzv. Site Survey software.

Úkol číslo 8

Maximální vyzářený výkon bezdrátového spoje může být roven?

4.3 Typy antén

Obecně o anténách

Nezbytnou součástí vybavení pro bezdrátové připojení jsou antény. Pro pokrytí bytu či kanceláře většinou postačují malé anténky, které jsou přibaleny k samotným kartám nebo přístupovým bodům, pro venkovní spoje, obzvlášť na delší vzdálenosti, už ale nestačí. Rušení, vliv počasí a překážky v cestě mají na signál neblahý vliv. Pak je třeba použít výkonnější anténu.

Vlastnosti antén vystihují některé důležité parametry, se kterými je třeba se na začátek seznámit. Ani zde tak vždy neplatí ono známé „čím větší, tím lepší". Antény se liší nejen tvarem podle účelu použití, ale také schopností zachytit slabší signál či způsobem šíření signálu.

Dělení antén

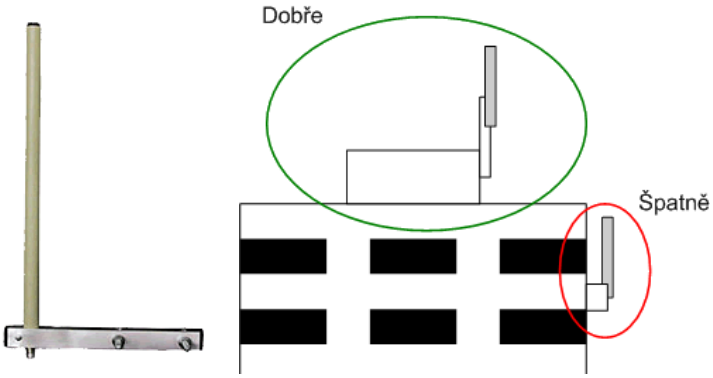
Základní rozdíl mezi anténami určující jejich použití spočívá ve směru, do kterého vysílají signál. Podle toho rozlišujeme antény trojího typu:

- **všesměrové antény** – vysílají do všech stran, tzn., že pokryjí úhel 360°. Běžně se dodávají ke všem Wi-Fi výrobkům. Například přístupový bod připojuje klienty ze všech směrů nebo síť ad-hoc propojuje vzájemně počítače po celém bytě ze všech směrů;
- **sektorové antény** – pokryjí jen určitý úhel od 30° do 180°. Jejich použití je vhodné tam, kde stačí pokrýt jen omezené území – například do rohu místnosti postačí anténa s 90° pokrytím. Můžete též s jejich pomocí zamezit šíření signálu (a potažmo možnosti přístupu do sítě) mimo žádané území;
- **směrové antény** – slouží k propojení dvou bodů na delší vzdálenosti, jelikož září jen do jednoho bodu. Používají se dva typy: parabolické, které mají drátěné síto a ozařovač uprostřed, a tzv. antény Yagi.

4.3.1 Všesměrové antény

Všesměrové antény

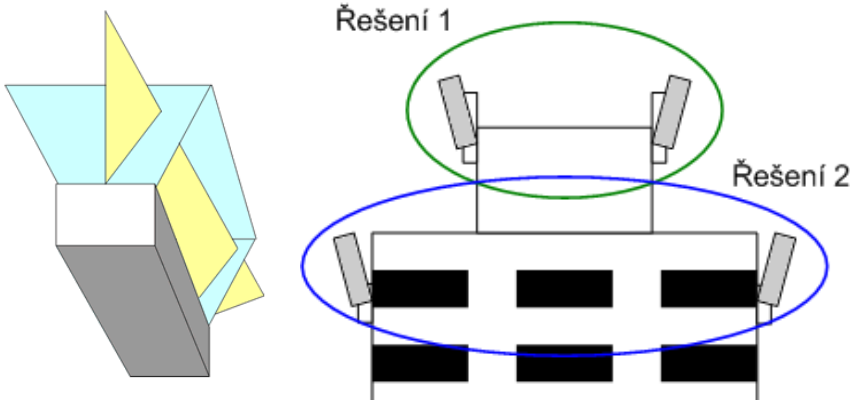
- Vyzařují signál horizontálně v rozsahu 360°, to znamená do všech stran.
- Vertikální vyzařování se pohybuje většinou okolo 15°.
- Nižší zisk antény.



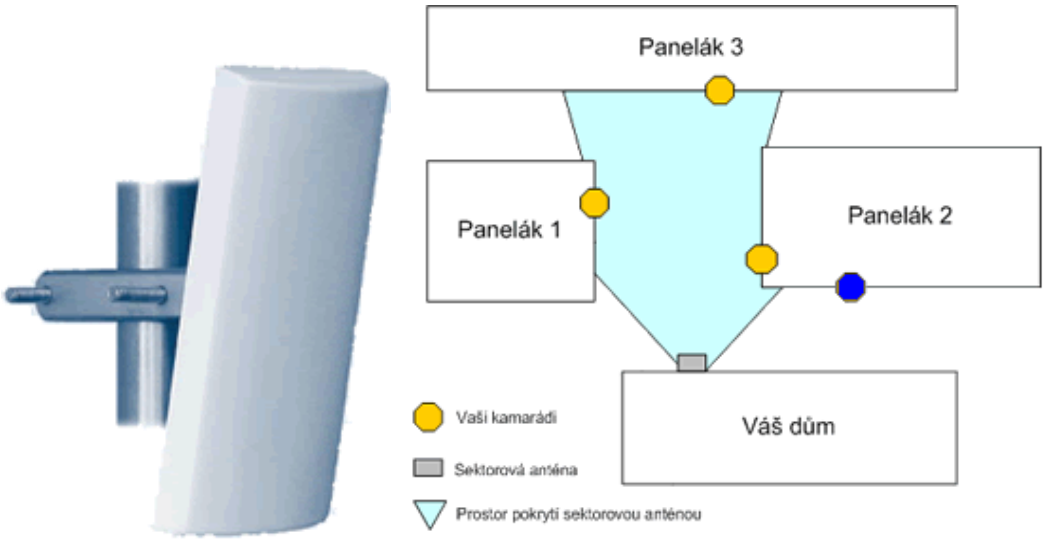
4.3.2 Sektorové antény

Sektorové antény

Vyzařují do určitého úhlu, například vykrývají úhel 180° nebo jen 60°. Používají se tam, kde je potřeba vykrýt specifické omezené oblasti a je Potřeba zabránit pronikání signálu mimo tuto oblast.



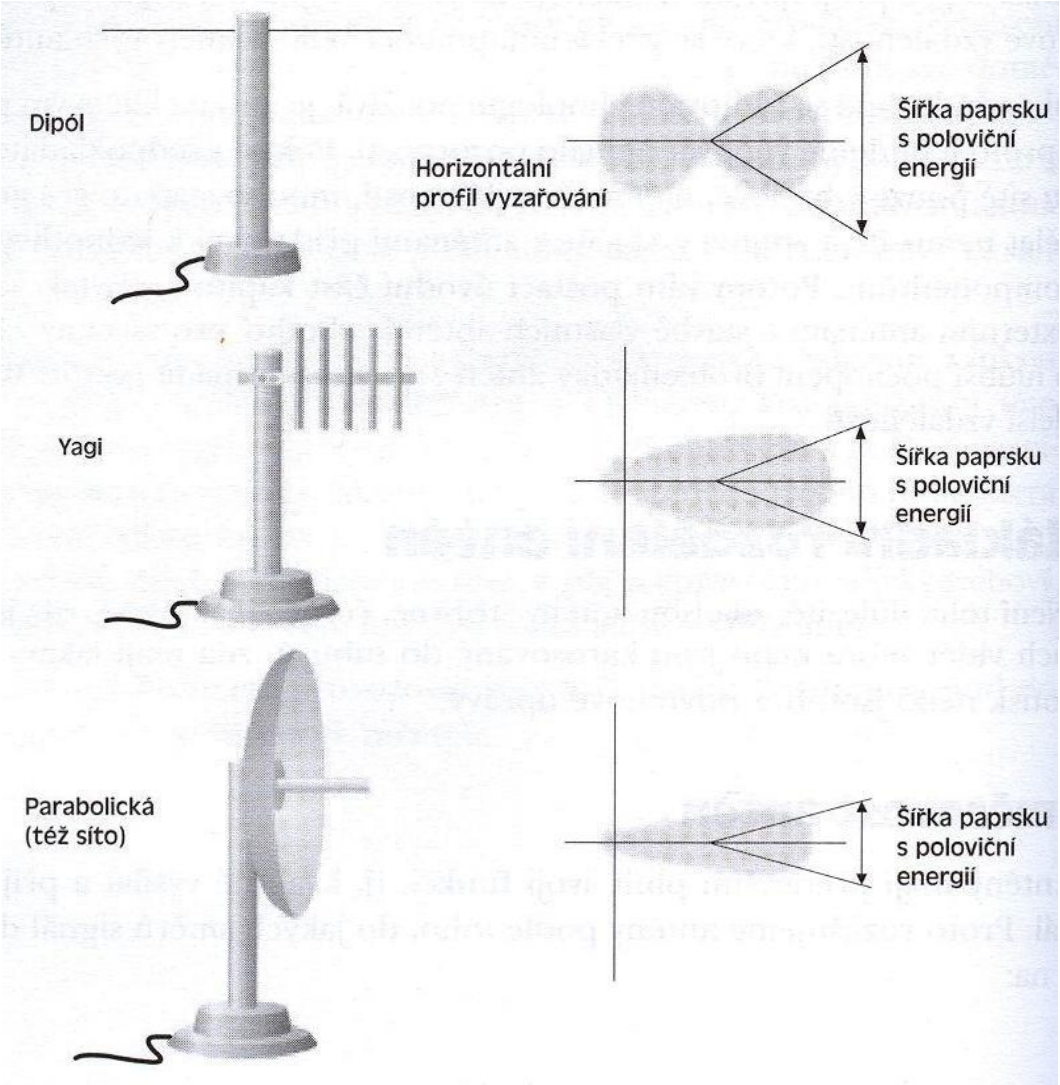
použití jako externí antény pro přístupové body.



4.3.3 Směrové antény

Směrové antény

Tyto antény září pouze do jednoho bodu a jsou to nejčastěji používané antény na delší spoje.



Pro zájemce

Pokud se vám nechce dávat tisíce korun za profesionální anténu a máte dostatek trpělivosti i zručnosti a děláte spoj na kratší vzdálenost, mohla by vám podomácku vyrobená anténa stačit.

Ačkoli by se mohlo zdát, nejde o složitou operaci. Jedna věc je však velmi důležitá – přesnost. Pokud vám tuhle ujede milimetr, tuhle druhý, může se stát, že anténa bude mít mnohem nižší zisk a zářit úplně jinam, než chcete. Návodů na stavbu Wi-Fi antén existuje spousta. Populární jsou antény typu Quad a Yagi, ale nejjednodušší je výroba tzv. kantény, neboli antény z plechovky (z angl. can).

Běžně se používají plechovky od párků (vhodné rozměry mají Kostelecké párky). Lze použít i jinou plechovku, ale pak je třeba přepočítat rozměry (viz odkazy). Ideální jsou plechovky s průměrem okolo 85 mm.

Vyrobit si vlastní kanténu není vůbec složité. Taková kanténa vás vyjde ani ne na 150 Kč a její výroba zabere tři hodiny času.

Plechovku nejprve pečlivě očistěte od mastnoty a nečistot a opilujete její ostrý okraj. Do plechovky pak vyvrtejte ve vzdálenosti 65 mm ode dna dírku, kterou postupně zvětšíte na průměr 8 mm. Poté do ní narazte F-konektor, který předtím zbavte matice. Konektor zapájejte a našroubujete do něj 75 ohmový satelitní koaxiální kabel tak, aby vnitřní měděný drát (může být i s dielektrikem) zasahoval do plechovky přesně 31 mm.

Porovnání plechovkových a komerčních antén				
anténa	10 db	11 db	24 db	kanténa
signál [db]	-83	-82	-67	-81
ruch/šum [db]	-92	-95	-102	-98

Pro zvýšení ziskovosti se antény opatřují ještě trychtýřem směřujícím více signálu do plechovky. Je vhodné opatřit otvor plastovým víčkem, které předtím otestujte v mikrovlnné troubě, jestli vlny opravdu propouští a nijak se nedeformuje. Víčko zabrání zatékání vody do plechovky. Konektor pak ze stejného důvodu zvenku zaizolujte silikonem nebo vyrobte vodotěsný kryt z PVC na celou anténu.

Takováto anténa je lineárně polarizovaná. Pokud jí při zaměřovaní budete otáčet podle osy, budete zvyšovat, resp. snižovat sílu signálu. Také je vhodné ji nasměrovat mírně na stranu k přípojnému bodu. Existují i další způsoby, jak „ladit" funkčnost takovéto antény – například změnou vzdálenosti konektoru ode dna (přidáním víčka plechovky na dno a pohybem s ním) či změnou celkové výšky antény pomocí konektoru.

4.4 Základní parametry antén

V předchozím textu jsem vás seznámil s některými pojmy, které souvisejí s možností instalace a provozu antén bezdrátových sítí postavených na technologii WiFi. V této části textu Vám tedy některé z těchto pojmů vysvětlím.

4.4.1 Zisk

Zisk antén

Dalším důležitým parametrem antén je zisk. Všechny antény jsou ve své podstatě směrové a míru směrovosti udává zisk, jenž je největší právě ve směru, kam anténa vyzařuje. Čím je vyšší, tím vzdálenější signál je schopna anténa zachytit.

Jedná se o poměr mezi intenzitou vyzařování v daném směru k intenzitě, kterou bychom obdrželi, kdyby energie přijatá anténou byla vyzářena rovnoměrně do všech směrů. Tak vyzařuje referenční, tzv. izotropní anténa, která ale existuje pouze na papíře, tudíž je nahrazována anténou dipólovou. Zisk je pak udáván v jednotkách dBi či dBd podle typu antény, vůči které je vztažen.

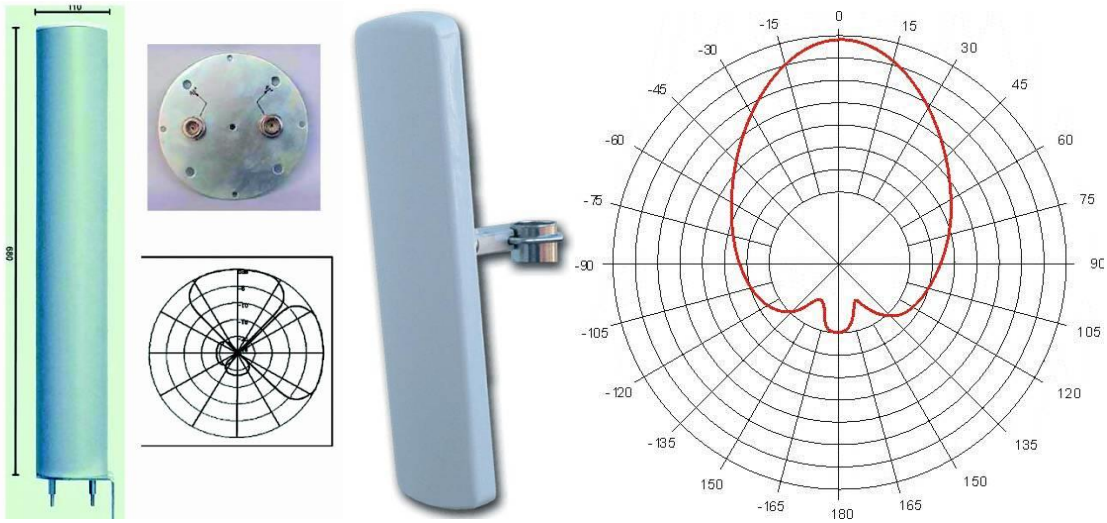
4.4.2 Vyzařovací úhly a diagramy

Úhly a vyzařovací diagramy

Vyzařovací úhly (horizontální a vertikální) udávají, jaký úhel před sebou a pod sebou je anténa schopna spolehlivě pokrýt.

Například všesměrová anténa má horizontální úhel 360°, sektorová třeba 45°, ale ve vertikálním úhlu je to již jen 30°. Takovou anténu proto nemůžete posadit na střechu domu a čekat, že pokryje vše pod sebou.

Zisk, směrovost a vyzařovací úhly antén jsou detailně zakreslovány do vyzařovacích diagramů. Ty ukazují plnou charakteristiku šíření signálu, jak horizontálně, tak vertikálně. Lze z nich vyčíst také odchylky oproti udávanému vyzařování, kdy anténa září i do postranních a zadních laloků.



Obrázky popisují:

- Sektorová anténa pokrývající úhel 23° až 60°, viz vyzařovací diagram Tato sektorová anténa se dvěma zářiči ozařuje úhel dvakrát 90°.
- Sektorová anténa ozařující 65°. Všimněte si v diagramu laloků za anténou.

4.4.3 Polarizace

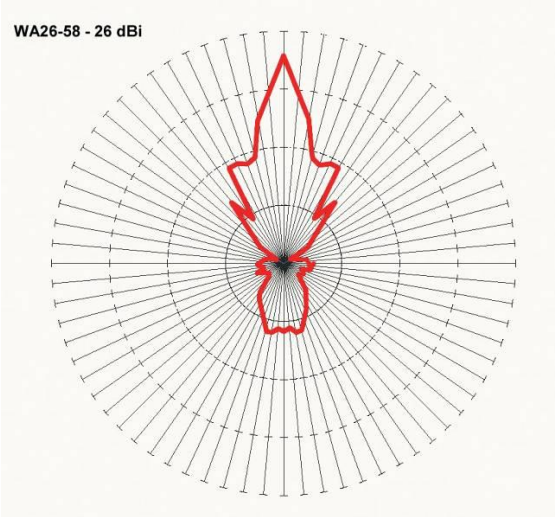
Polarizace antén

Polarizace udává rovinu, ve které se šíří rádiové vlny. Pro optimální spojení musí být na obou stranách antény se stejnou polarizací. V opačném případě dochází k velikým ztrátám a potlačení zisku antén až o 16–24 dB, což v důsledku znemožní přenos dat.

Z pohledu polarizace rozeznáváme tři typy antén:

- lineární horizontální – je vhodná na delší spoje bod-bod;
- lineární vertikální – používá se na připojení klientů k přístupovému bodu;
- kruhová – antény s touto polarizací se používají tam, kde kvůli velkému zarušení už není možno použít anténu lineární.

Změna polarizace se dá využít v zarušeném prostředí k potlačení rušení od ostatních sítí. Ke změně horizontální na vertikální stačí otočit zářič o 90°.



4.4.4 Jak si vybrat správnou anténu?

Výběr antény

Ačkoli lze určit dosah antén v nezarušeném prostředí, v reálném světě bude situace značně odlišná. Některé městské aglomerace například trpí takovým zarušením, že vybudovat v nich další bezdrátové spoje je dnes téměř nemožné. Určit, jakou anténu budete potřebovat právě vy, proto není tak jednoduché. Pro představu se podívejte, jaké vzdálenosti je možné docílit v nezarušeném prostředí připojením typu bod-bod s anténou o zisku 36 dBm na jedné straně a klienty s různým ziskem na straně druhé.

Dosažitelné vzdálenosti s anténou o zisku 36 dBm o různém zisku	
Vzdálenost [km]	Zisk [dBi]
0,8–3	7–9
3–8	9–15
8–11	15–20
11+	20–24

Anténky dodávané k Wi-Fi zařízením mají zisk jen 1–2 dBi. V otevřeném nezarušeném prostoru se sice spojí i na vzdálenost 300 m, uvnitř budov však již maximálně na 30 m. Signál je zde už silně tlumen zdmi a také rušen jinými zařízeními či kabelovými rozvody. Už dvě železobetonové zdi panelového domu dokáží signál z těchto antén naprosto utlumit. Lépe jsou na tom cihlové zdi a nejlépe pak kartónové.

http://www.zive.cz/files/obrazky/2005/9/anteny/yagi1.jpg

- Všesměrová 12dBi anténa OMNI12 má vertikální vyzařovací úhel jen 8°
- Všesměrová 8dBi anténa OMNI8 má vertikální vyzařovací úhel jen 8°
- Směrová anténa typu Yagi

Podle čeho tedy vybírat? Ujasněte si, k jakému účelu budete anténu používat.

- Bude to spojení na jeden, nebo vícero bodů?
- Jaký úhel je třeba pokrýt?
- Jaký typ polarizace se bude používat?

Ziskovost antény pak odhadněte podle tabulky nebo se poraďte se svým budoucím poskytovatelem připojení (internetového přes Wi-Fi nebo komunitní síť), který by měl být schopen proměřit situaci právě ve vašem bydlišti.

Úkol číslo 9

Z pohledu polarizace rozeznáváme kolik typů antén?

Shrnutí

- Vysílaná informace jde z vysílače do antény, následně pak v podobě elektromagnetických vln vzduchem do přijímače, kde je informace demodulována do své původní podoby.
- Pro libovolný výpočet je nutné znát používané jednotky a definici souvisejících parametrů. Prvním z nich je **výstupní úroveň vysílače** a **vstupní úroveň přijímače**.
- V České republice je maximální výstupní úroveň omezena Generálním povolením ČTÚ č. 01/1994 na 100 mW EIRP, tzn. 20dBm.
- Útlum závisí na takových parametrech, jako je: vícecestné šíření signálu, přímá viditelnost, počasí, např. vítr, déšť, rušení s jinými systémy ve stejném pásmu.
- Je však třeba říci, že vliv počasí je minimální. Například i velmi intenzivní déšť 150 mm/h způsobí zeslabení signálu maximálně o 0,02 dB/km. Mnohem významnější jsou pak nepřímé vlivy, jako je např. mokré listí na stromech, které de facto vytváří "vodní stěnu". Voda vlny v pásmu 2,4 GHz nepropouští – mění je na tepelnou energii.
- Parametry, které jsme si jmenovaly v předchozí části, způsobují **ztráty na přenosové trase**. Jedná se o ztrátu energie během přenosu rádiového signálu vyjádřenou v dB. Tyto ztráty jsou závislé mimo výše uvedeného na následujících faktorech: vzdálenost mezi přijímací a vysílací anténou; přímá viditelnost mezi příjímací a vysílací anténou; vlastní parametry použité antény.
- Důležité je si uvědomit, co se myslí pojmem **přímá viditelnost**. Protože se nejedná o laser, nestačí nám optická přímá viditelnost, ale potřebujeme i určitý prostor kolem. Jedná se o tzv. **Fresnelovou zónu.**
- Jedním z nejdůležitějších prvků na kterém závisí kvalita spoje je **anténa**. Anténu zpravidla definujeme jako prvek, který umožňuje přechod elektromagnetického vlnění přiváděného na elektromagnetické vlnění ve volném prostoru.
- Jedním ze základních pojmů je **izotropní anténa**. Jde o bod, který rovnoměrně vyzařuje do všech směrů (360°) a to beze ztrát. Jedná se o teoretickou, tj. technicky nerealizovatelnou anténu, která slouží pro výpočty a popis parametrů skutečných antén.
- Pomocí izotropní antény se definuje např. **zisk antény**. Jedná se o poměr mezi intenzitou vyzařování v daném směru k intenzitě vyzařování, kterou bychom obdrželi, kdyby energie přijatá anténou byla vyzářena rovnoměrně do všech směrů. Zisk antény se udává v dBi.
- Zisk antény úzce souvisí se **směrovostí** a následně pak s dosahem. Tato souvislost je nejlépe patrná při grafickém znázornění **vyzařovací charakteristiky.**
- Poslední dva parametry, které potřebujeme znát, jsou **útlum kabelu** a **citlivost přijímače**. Útlum kabelu je dán typem kabelu. Obyčejný RG-58, koaxiální kabel používaný mj. i pro

Ethernet, má útlum 1 dB/m. U kabelu RG-214 je to 0,6 dB/m a u speciálního kabelu typu Heliax pouze 0,11 dB/m. Citlivost přijímače je nutné zjistit u výrobce daného zařízení.

- **Zásadní omezení je dáno Generálním povolením ČTÚ č. 01/1994 které říká, že maximální vyzářený výkon může být 100 mW EIRP**. Pro zvětšení dosahu lze použít různé zesilovače, ale vždy pouze v souladu s výše uvedeným povolením.
- Nezbytnou součástí vybavení pro bezdrátové připojení jsou antény. Pro pokrytí bytu či kanceláře většinou postačují malé anténky, které jsou přibaleny k samotným kartám nebo přístupovým bodům, pro venkovní spoje, obzvlášť na delší vzdálenosti, už ale nestačí. Rušení, vliv počasí a překážky v cestě mají na signál neblahý vliv. Pak je třeba použít výkonnější anténu.
- Vlastnosti antén vystihují některé důležité parametry, se kterými je třeba se na začátek seznámit. Ani zde tak vždy neplatí ono známé „čím větší, tím lepší". Antény se liší nejen tvarem podle účelu použití, ale také schopností zachytit slabší signál či způsobem šíření signálu
- Základní rozdíl mezi anténami určující jejich použití spočívá ve směru, do kterého vysílají signál. Podle toho rozlišujeme antény trojího typu: **všesměrové antény** – vysílají do všech stran, tzn., že pokryjí úhel 360°. Běžně se dodávají ke všem Wi-Fi výrobkům. Například přístupový bod připojuje klienty ze všech směrů nebo síť ad-hoc propojuje vzájemně počítače po celém bytě ze všech směrů; **sektorové antény** – pokryjí jen určitý úhel od 30° do 180°. Jejich použití je vhodné tam, kde stačí pokrýt jen omezené území – například do rohu místnosti postačí anténa s 90° pokrytím. Můžete též s jejich pomocí zamezit šíření signálu (a potažmo možnosti přístupu do sítě) mimo žádané území; **směrové antény** – slouží k propojení dvou bodů na delší vzdálenosti, jelikož září jen do jednoho bodu. Používají se dva typy: parabolické, které mají drátěné síto a ozařovač uprostřed, a tzv. antény Yagi.
- Vyzařovací úhly (horizontální a vertikální) udávají, jaký úhel před sebou a pod sebou je anténa schopna spolehlivě pokrýt. Například všesměrová anténa má horizontální úhel 360°, sektorová třeba 45°, ale ve vertikálním úhlu je to již jen 30°. Takovou anténu proto nemůžete posadit na střechu domu a čekat, že pokryje vše pod sebou.
- Zisk, směrovost a vyzařovací úhly antén jsou detailně zakreslovány do vyzařovacích diagramů. Ty ukazují plnou charakteristiku šíření signálu, jak horizontálně, tak vertikálně. Lze z nich vyčíst také odchylky oproti udávanému vyzařování, kdy anténa září i do postranních a zadních laloků.
- Polarizace udává rovinu, ve které se šíří rádiové vlny. Pro optimální spojení musí být na obou stranách antény se stejnou polarizací. V opačném případě dochází k velikým ztrátám a potlačení zisku antén až o 16–24 dB, což v důsledku znemožní přenos dat.
- Z pohledu polarizace rozeznáváme tři typy antén: lineární horizontální – je vhodná na delší spoje bod–bod; lineární vertikální – používá se na připojení klientů k přístupovému bodu; kruhová – antény s touto polarizací se používají tam, kde kvůli velkému zarušení už není možno použít anténu lineární.

Kontrolní otázky a úkoly

1. Charakterizujte všesměrové antény.
2. Popište funkci směrové antény.
3. Jaké další tyty antén znáte?
4. Co znamená útlum?
5. Co znamená zisk?
6. Co definuje Fresnelova zóna?
7. Uveďte základní typy rušení a ztrát na trase.
8. Charakterizujte izotropní anténu.

Pojmy k zapamatování

Anténa, útlum, zisk antény, Fresnelova zóna, izotropní anténa, směrová anténa, všesměrová anténa, sektorová anténa.

Literatura

Základní:
ZANDL, P. *WiFi – praktický průvodce.* 1. vyd. Brno: Vydavatelství Computer Press, 2003. 217 s. ISBN 80-7226-632-2.
KÖHRE, T. *Stavíme si bezdrátovou síť Wi-fi* [překlad Marek Šiller]. Vyd. 1. vyd, Brno: Vydavatelství Computer Press, 2004. 295 s. ISBN 80-251-0391-9.

Rozšířená (pro hlubší pochopení):
DAVIS, H. *Průvodce úplného začátečníka pro Wi-Fi bezdrátové sítě: není zapotřebí žádných předchozích zkušeností!* [přeložil Karel Voráček]. 1. vyd. Praha: Vydavatelství Grada, 2006. 334 s. ISBN 80-247-421-3.

Průvodce studiem

Pokud se vám zdá, že zapomínáte to, co jste se naučili v předchozích kapitolách tak nezoufejte. To je normální průvodní jev při učení. Jak se sami přesvědčíte, ke zopakování Vám však bude tentokrát stačit o mnoho méně času.

Doporučujeme Vám nepodceňovat kontrolní otázky uvedené vždy v závěrech kapitol. Dotazují se na základní učivo, které je potřebné znát.

Nepodceňujte význam relaxace a odpočinku. Rychlé memorování nelze považovat za efektivní metodu učení a vědomosti nejsou trvalé. To jistě ale víte a proto se učíte průběžně.

5 Hardware pro WiFi sítě – Konektory, kabely a bleskojistky

Cíle

Po prostudování této kapitoly byste měli být schopni:

- charakterizovat pojem konektor,
- rozčlenit konektory do základních skupin,
- uvést základní propojovacích kabelů,
- popsat princip činnosti bleskojistky,
- popsat složení propojovacího kabelu,
- určit rozdíl mezi levnými a drahými kabely,
- popsat fyzické zapojení bleskojistky.

Průvodce studiem

Takže už znáte základní pojmy z bezdrátových sítí (případně si je dle potřeby naleznete v některém ze slovníků výpočetní techniky), víte též, jak bezdrátová síť funguje. K tomu jsme postupně přidali poznatky o přístupových bodech a anténách. Taktéž jsme se naučili jak postupovat při studiu. Následovat by měl zasloužený konec, ale ještě tomu tak nebude.

Je potřeba Vás pochválit, jelikož jestliže jste postoupili až k této poslední kapitole, máte dobře vykročeno k úspěšnému absolvování předmětu.

Posledním článkem pomyslného řetězu jsou konektory a propojovací kabely, které umožní z oddělených prvků bezdrátové sítě vytvořit jeden funkční celek. Podívejme se tedy společně na tuto problematiku.

Potřebný čas pro studium kapitoly:

- 30 minut

5.1 Konektory

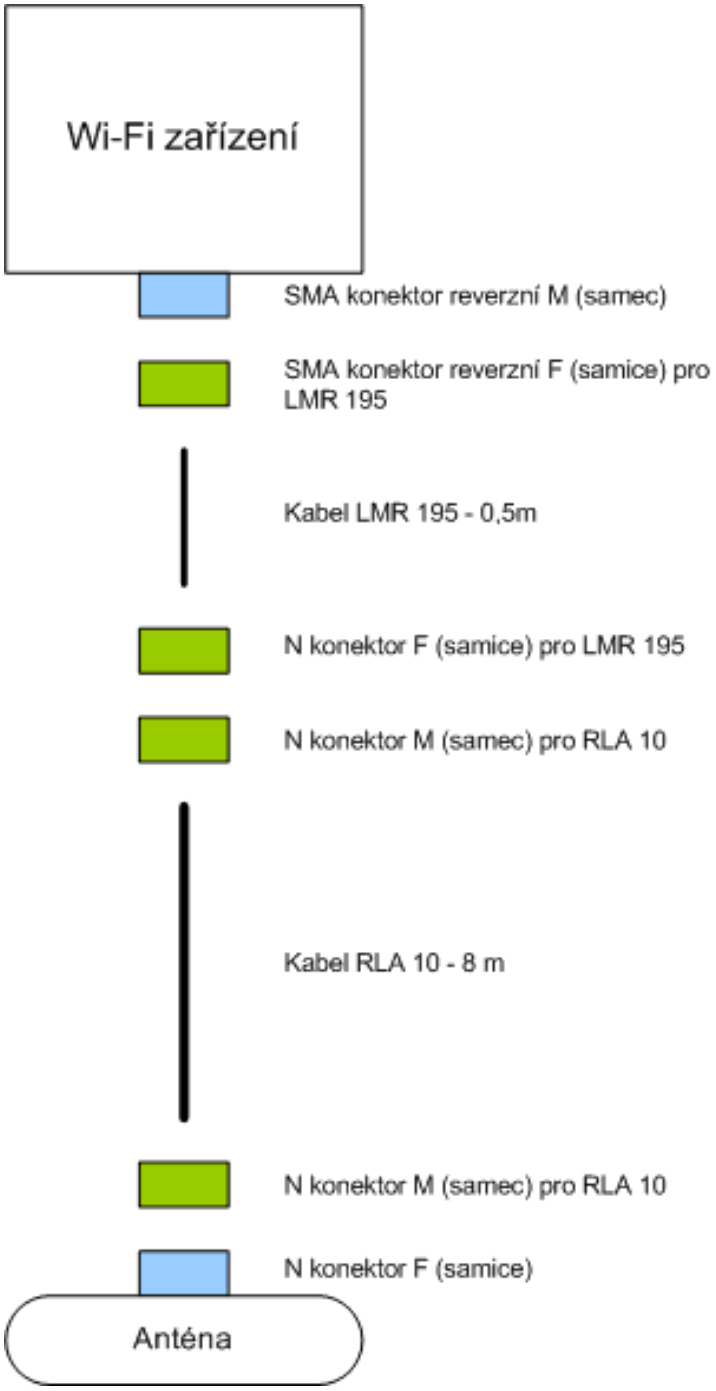
Konektory slouží ke spojení vybraného kabelu s Wi-Fi zařízením, s externí anténou a nebo mezi kabely samými. Výběr konektoru je o trochu složitější než výběr kabelu a je nezbytně nutné znát následující údaje:

- Výstupní konektor vašeho Wi-Fi zařízení – nejběžnější je SMA konektor, který se nachází na většině interních PCI karet a Access pointech. Výjimku tvoří společnosti Avaya a Orinoco, které používají konektor "Mini", či Linksys, který na svých přístupových bodech používá konektor TNC. Typ konektoru ale není to jediné, co musíte v dokumentaci od výrobce nalézt. Je velice důležité zjistit, jestli je konektor samec (Male) či samice (Female), dále jestli se jedná o konektor reverzní či nikoli.
- Výstupní konektor na vaší anténě – ve většině případů je použit N konektor ve verzi samice, ale existují i výjimky, kde jsou užity konektory samci.
- Typ vašeho kabelu

Pokud zjistíte všechny potřebné informace o konektorech na vašem Wi-Fi zařízení a anténě, nic nebrání tomu, abyste zakoupili k nim **OPAČNÉ** konektory, kompatibilní s vaším kabelem.

Ukázkové zapojení:

Struktura zapojení



Konektory jsou krimpovací, to znamená, že je můžete pomocí speciálních kleští BNC HT(336A) jednoduše „nacvakat" na kabel sami. Avšak doporučují se letovat.

Tvary konektorů

Pochopitelně existují i různé spojky jako N samce na N samice a další. Pro vysokofrekvenční digitální techniku se nejčastěji používají konektory typu N nebo SMA. Jeden pár N konektorů má typicky útlum 1 dB, pár SMA konektorů cca 0,1 – 0,5 dB. Konektory typu N (vyrábějí se již od roku 1943 a jsou vyhovující až do frekvence 10 GHz) jsou velice robustní a používají se nejčastěji pro venkovní aplikace (spoje kabelů, antény). Konektory typu SMA se používají v aktivních prvcích a nejsou projektovány pro venkovní použití.

N konektory

N konektory se vyrábějí v mnoha variantách a kvalitách. Mohou být buď šroubovací (na kabel se připevňují šroubováním matky, která uvnitř konektoru stlačí gumové těsnění a přitiskne stínění kabelu k plášti konektoru) nebo krimplovací, což znamená, že speciálními krimplovacími kleštěmi zalisujeme stínění koaxiálního kabelu mezi konektor a krimplovací kroužek. Druhá metoda se v praxi osvědčila jako levnější, rychlejší a spolehlivější.

Nejkvalitnější profesionální konektory vyrábí firma Aircom, jeden konektor vychází na cca 400 Kč a lze je používat bez jakékoliv další úpravy i pro vnější prostředí (jsou vodotěsné, nekorodující, záruka 10 let).

Každý konektor je potřeba po montáži proměřit proti zkratu a zaizolovat proti povětrnostním vlivům. Nejčastěji se na to používá tzv. samovulkanizační páska, což je lepicí páska ze speciální hmoty, která se po aplikaci "slije" do jednoho celku a dokonale zaizoluje spoj. Tuto pásku koupíme buď přímo u prodejců Wi-Fi techniky, nebo v elektroinstalačních potřebách.

Některé konektory (SMA, RSMA) se však vůbec na tlusté 11 mm kabely nevyrábějí a je proto potřeba používat redukce (tzv. pigtaily). Tyto redukce se vyrábějí pouze z tenkých a ohebných kabelů v délce cca 25 cm a slouží pro propojení tlustého koax. kabelu vedoucího od antény s aktivním Wi-Fi prvkem.

5.2 Kabely

Útlum kabelu

Rozhodujícím faktorem pro použití určitého typu kabelu je jeho útlum. Ten je vždy vztažen k pracovnímu kmitočtu a jednotkové délky. Uvádí se tedy např. v dB/100 m při nějakém kmitočtu. Obecně platí, že silnější „koax" (tedy s větším průměrem) mívá nižší útlum.

Struktura kabelu

Konstrukčně je kabel uspořádán tak, že je tvořen středním vodičem, dielektrikem, vnějším stíněním a ochranným pláštěm. Střední vodič bývá buď plný, někdy i licna (lanko).

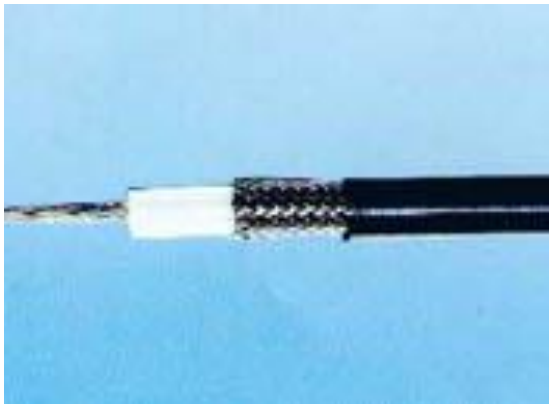
Dielektrikum může být polyetylenové (PE), pěnové, teflonové (PTFE), někdy i vzdušné nebo kombinované. U kabelů se vzdušným či kombinovaným dielektrikem bývá střední vodič fixován ve správné poloze např. pomocí korálků, polyetylenovou hvězdičkou apod.

Dielektrikum

Vnější stínění je většinou provedeno jako měděné opletení, které může být někdy dvojité. Stínění se vyskytuje rovněž postříbřené či stříbrné, někdy ho může tvořit měděná trubka, která může být také zvlněná. Vyskytují se rovněž kombinace opletené a fólie apod.

Konstrukční uspořádání kabelu má velký vliv na jeho útlum, levné kabely mívají pouze jednoduché stínění tvořené jednovrstvým opletením.

Levné kabely s jednoduchým stíněním:



Kvalitnější kabely používají fólii kombinovanou s opletením:

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

Velkou nevýhodou u tlustých 11 mm kabelů je horší dostupnost VF konektorů a jejich vyšší cena. Často ani není možné na tyto kabely sehnat správné konektory pro Wi-Fi techniku a proto se tento problém řeší různými redukcemi a propojkami (slangově nazývanými pigtaily), které zvyšují útlum a poruchovost celého anténního systému.

Pokud nepotřebujeme překonávat velké vzdálenosti (do 10 m), často místo 11 mm tlustých a neohebných kabelů volíme jejich tenčí, 5 mm ekvivalenty. Jsou to především kabely od firem Andrew a TimesMicrowave typu 195 (CNT-195, LX-195, LMR-195).
Tyto kabely mají stejný rozměr jako kabel RG58, jsou však projektovány pro vyšší frekvence a jejich útlum se při 2,4 GHz pohybuje okolo hodnoty 0,5 dB/m. Velká výhoda tenkých 5 mm kabelů je široká dostupnost všech druhů konektorů pro tyto kabely (např. RSMA konektory, TNC, SMA atd.) a proto je tendence používat tyto kabely všude kde je to možné.

Většina dostupné Wi-Fi techniky deklaruje výstupní impedanci (zjednodušeně řečeno: stálý poměr mezi induktancí a kapacitancí zaručující stejné chování kabelu při libovolné délce) na úrovni 50 ohmů a proto se všeobecně doporučuje používat pouze 50 ohmové kabely. Praktickým měřením jsme však zjistili, že výstupní impedance Wi-Fi prvků se pohybuje od 30 do 70 ohmů v závislosti na konkrétním kuse a značce. Navíc útlum vzniklý impedančním nepřizpůsobením mezi 50 a 75 ohmovým kabelem je pouze cca 4% a proto je možné pro Wi-Fi aplikace používat jakýkoliv kvalitní 75 ohmový kabel bez měřitelné ztráty kvality (např. velice kvalitní 75 ohmový kabel Belden H125).

Koaxiální kabely vedeme nejkratší možnou cestou, bez prudkých ohybů (každý koax. kabel má ve své specifikaci minimální poloměr ohybu), kroucení, smyček atd. V žádném případě neomotáváme koax. kabel okolo žádných kovových trubek ani nepoužíváme kovové průchodky. Pokud máme anténu na stožáru, v žádném případě nevedeme koax. kabel vnitřkem stožárové trubky, ale pouze po okraji a nejlépe alespoň v 1 cm vzdálenosti (potřebné objímky lze zakoupit v elektroinstalačních potřebách).
Koaxiální kabely zakončujeme nejčastěji konektory typu N nebo SMA. N konektory se používají na anténách, SMA nebo reverzní SMA (obrácená polarita) se používají na aktivních prvcích.

Úkol číslo 10

Konstrukčně je kabel uspořádán tak, že je tvořen?

5.3 Bleskojistky

Přepěťová ochrana neboli zkráceně bleskojistka slouží k ochraně aktivních prvků bezdrátové sítě před atmosférickou elektřinou.
V ideálním případě se instaluje do místa, kde koaxiální vedení přechází z vnitřních do vnějších prostor. Instalující se většinou mezi dva N samce konektory. Proti přímému zásahu vám pravděpodobně moc nepomůže, ale díky základní ochraně proti přepětí a atmosférickým výbojům vám může ušetřit hodně starostí, pokud blesk udeří opodál. Bleskojistky existují s pásmovou propustí a lepší plynové. Při jejich použití dávejte pozor na útlum a počítejte s -0.5 dB.

Pro potřeby Wi-Fi je jediným vyhovujícím způsobem ochrany před přepětím pásmová propusť. Pracuje na jednoduchém principu – jedná se o laděný rezonátor, který zkratuje veškeré frekvence mimo jediné pracovní, v našem případě 2,4 GHz. Kvalitní přepěťové ochrany odolají přímému zásahu blesku a jsou testovány nárazem proudové vlny o amplitudě 3 kA a době trvání 350 µs.

Shrnutí

- Konektory slouží ke spojení vybraného kabelu s Wi-Fi zařízením, s externí anténou a nebo mezi kabely samými.
- Konektory jsou krimpovací, to znamená, že je můžete pomocí speciálních kleští BNC HT(336A) jednoduše „nacvakat" na kabel sami. Avšak doporučují se letovat.
- Pro vysokofrekvenční digitální techniku se nejčastěji používají konektory typu N nebo SMA. Jeden pár N konektorů má typicky útlum 1 dB, pár SMA konektorů cca 0,1 – 0,5 dB.
- Nejkvalitnější profesionální konektory vyrábí firma Aircom, jeden konektor vychází na cca 400 Kč a lze je používat bez jakékoliv další úpravy i pro vnější prostředí (jsou vodotěsné, nekorodující, záruka 10 let).
- Každý konektor je potřeba po montáži proměřit proti zkratu a zaizolovat proti povětrnostním vlivům. Nejčastěji se na to používá tzv. samovulkanizační páska, což je lepicí páska ze speciální hmoty, která se po aplikaci "slije" do jednoho celku a dokonale zaizoluje spoj.
- Rozhodujícím faktorem pro použití určitého typu kabelu je jeho útlum. Ten je vždy vztažen k pracovnímu kmitočtu a jednotkové délky. Uvádí se tedy např. v dB/100 m při nějakém kmitočtu. Obecně platí, že silnější „koax" (tedy s větším průměrem) mívá nižší útlum.
- Konstrukčně je kabel uspořádán tak, že je tvořen středním vodičem, dielektrikem, vnějším stíněním a ochranným pláštěm. Střední vodič bývá buď plný, někdy i licna (lanko).
- Velkou nevýhodou u tlustých 11 mm kabelů je horší dostupnost VF konektorů a jejich vyšší cena. Často ani není možné na tyto kabely sehnat správné konektory pro Wi-Fi techniku a proto se tento problém řeší různými redukcemi a propojkami (slangově nazývanými pigtaily).
- Pokud nepotřebujeme překonávat velké vzdálenosti (do 10 m), často místo 11 mm tlustých a neohebných kabelů volíme jejich tenčí, 5 mm ekvivalenty. Jsou to především kabely od firem Andrew a TimesMicrowave typu 195 (CNT-195, LX-195, LMR-195).
- Koaxiální kabely vedeme nejkratší možnou cestou, bez prudkých ohybů (každý koax. kabel má ve své specifikaci minimální poloměr ohybu), kroucení, smyček atd. V žádném případě neomotáváme koax. kabel okolo žádných kovových trubek ani nepoužíváme kovové průchodky.
- Přepěťová ochrana neboli zkráceně bleskojistka slouží k ochraně aktivních prvků bezdrátové sítě před atmosférickou elektřinou.

- V ideálním případě se instaluje do místa, kde koaxiální vedení přechází z vnitřních do vnějších prostor. Instalující se většinou mezi dva N samce konektory.
- Pro potřeby Wi-Fi je jediným vyhovujícím způsobem ochrany před přepětím pásmová propusť. Pracuje na jednoduchém principu – jedná se o laděný rezonátor, který zkratuje veškeré frekvence mimo jediné pracovní, v našem případě 2,4 GHz.

Kontrolní otázky a úkoly

1. Vysvětlete k jakému účelu slouží konektory.
2. Uveďte, do jakých základních skupin lze konektory rozdělit.
3. Popište základní parametry kabelů.
4. Vysvětlete princip bleskojistky.

Pojmy k zapamatování

SMA, RSMA, pigtail, N konektor, samovulkanizační páska, LMR kabel, bleskojistka, pásmová propusť.

Literatura

Základní:
ZANDL, P. *WiFi – praktický průvodce.* 1. vyd. Brno: Vydavatelství Computer Press, 2003. 217 s. ISBN 80-7226-632-2.
KÖHRE, T. *Stavíme si bezdrátovou síť Wi-fi* [překlad Marek Šiller]. Vyd. 1. vyd, Brno: Vydavatelství Computer Press, 2004. 295 s. ISBN 80-251-0391-9.

Rozšířená (pro hlubší pochopení):
DAVIS, H. *Průvodce úplného začátečníka pro Wi-Fi bezdrátové sítě: není zapotřebí žádných předchozích zkušeností!* [přeložil Karel Voráček]. 1. vyd. Praha: Vydavatelství Grada, 2006. 334 s. ISBN 80-247-421-3.

Průvodce studiem

Tak jsme to společně zvládli. Když si uvědomíte, že pokud se podrobněji bezdrátovými sítěmi zabýváte, musíte sami uznat, že jste udělali velký krok kupředu. Jenže to bohužel nestačí. V dalším studijním textu se proto budeme konkrétní konfigurací jednotlivých prvků bezdrátových sítí.

Kdykoliv při dalším studiu narazíte na něco, co si nepamatujete, snažte se co nejdříve mezery doplnit. Nemusíte již ale hluboce studovat, postačí k tomu již pouhé prolistování této, či jiné studijní opory.

Použitá literatura

ZANDL, P. *WiFi – praktický průvodce.* 1. vyd. Brno: Vydavatelství Computer Press, 2003. 217 s. ISBN 80-7226-632-2.

KÖHRE, T. *Stavíme si bezdrátovou síť Wi-fi* [překlad Marek Šiller]. Vyd. 1. vyd, Brno: Vydavatelství Computer Press, 2004. 295 s. ISBN 80-251-0391-9.

HORÁK, J. *Hardware*. 2. vyd. Brno: Computer Press, 1998, 331 s. ISBN 80-7226-122-3.

DAVIS, H. *Průvodce úplného začátečníka pro Wi-Fi bezdrátové sítě: není zapotřebí žádných předchozích zkušeností!* [přeložil Karel Voráček]. 1. vyd. Praha: Vydavatelství Grada, 2006. 334 s. ISBN 80-247-1421-3.

PELIKÁN, J. *Architektura počítačů PC.* Dostupné z: http://www.fi.muni.cz/usr/pelikan.

TOMAN, J. *Metody a techniky informační činnosti.* 1. vyd. Praha, SNTL, 1970. 214 s.

ZŮNA, P. *Informatika a výpočetní technika.* 1. vyd. Praha, Nakladatelství Grada, 1993, 184 s. ISBN 80-85623-63-3.