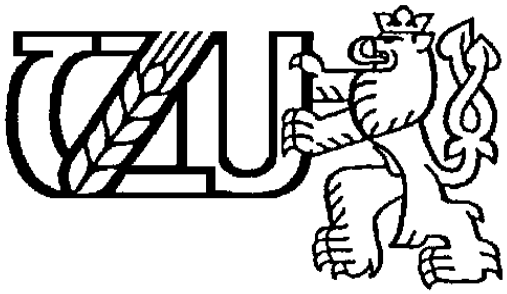
Česká zemědělská univerzita

Provozně ekonomická fakulta

Katedra informačních technologií



Bakalářská práce

Domácí počítačová síť

Household computer network

Autor bakalářské práce: Miroslav Krček

Vedoucí práce: RNDr. Eva Jablonská, CSc.

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně, pouze za odborného vedení vedoucího bakalářské práce RNDr. Evy Jablonské, CSc.

Dále prohlašuji, že veškeré podklady, ze kterých jsem čerpal jsou uvedeny v seznamu použitých zdrojů.

Miroslav Krček

Poděkování

Rád bych tímto poděkoval paní RNDr. Evě Jablonské, CSc. za vedení a odborné rady při tvorbě mé bakalářské práce.

1. Souhrn

V dnešní době, kdy je v domácnosti běžnou záležitostí více než jeden počítač, se stává samozřejmostí připojení k internetu. Proto logicky vyvstala potřeba vytvářet malé lokální sítě i v těchto místech. Jednou z možností jak tuto síť vytvořit, poskytuje bezdrátová technologie. Tato technologie je již na velmi vysoké úrovni a mnohdy poskytuje efektivnější prostředí než běžná LAN síť.

Cílem mojí práce je přiblížit tuto technologii běžnému uživateli a osvětlit mu základní terminologii této problematiky. Především jednotlivé typy standardu IEEE, a také směry nového vývoje. Dále je zde poukázáno na možnost ochrany těchto sítí i na nové směry ochrany proti vnějším útokům. To bývá stále ještě ve velkém množství případů, uživateli těchto sítí, zanedbáváno.V základní rovině je vysvětleno, jak takovouto sít postavit.

Tento popis je určen běžnému uživateli informačních technologií se základní počítačovou gramotností. Tato práce by měla tedy podat důležitou část této problematiky, která je podstatná pro uživatele, kteří jsou rozhodnuti si postavit bezdrátovou domácí počítačovou sít.

1.1. Summary

In these days, when are more than one computer common matter in household, internet connection is become apparent. Then discovered logical needs of small local network in these places. One of possibilities creating this network is providing wireless technology. This technology is at very high level and often provide more effective environment than common LAN network.

Target of my work bring this technology common user and explain him basic terminology of this problems. First of all are individual types of standard IEEE and direction of new development too. So, in this work is refer to protection these networks and new directions protections against outside attacks. It is still being in big quantity causes neglected by users of these networks. In basic level is explain, how build this network.

This description is determined for common user information technology with basic computer's literacy. This work should give important part of this problematic, which is important for users, whose are decided build their home wireless network.

1.2. Klíčová slova

IEEE 802.11, WiFi, WLAN, WEP, WPA, WPA2, WDS, ad-hoc, bezdrátová technologie, stavba bezdrátové LAN.

1.3. Key words

IEEE 802.11, WiFi, WLAN, WEP, WPA, WPA2 , ad-hoc WDS, wireless technology, construction wireless LAN.

2. Úvod

V dnešní době poskytuje domácí počítačová síť mnohé nové možnosti při jejich zavádění do domácností a v jejich využití v rodině. Ať už se jedná o klasické ethernetové propojení kabely či dnes již mnohem inovativnější bezdrátové propojení lokální sítě. Nicméně rozvoj sítí je v domácnostech čím dál větší. Email, chat, videokonference a především internetová telefonie je dnes hodně využívaným prostředkem komunikace.

Důvodem výběru tohoto tématu byla nastupující doba výhod bezdrátových sítí v domácnostech oproti klasické drátové LAN síti, která se v určitých situacích jeví jako velice nepraktická a velmi nákladná, hlavně v místech, kde by bylo zapotřebí takovýto kabel nákladným způsobem zavést do domácnosti. Pomocí radiových vln je tedy takovýto problém vyřešen daleko výhodněji. Technika většinou v dnešní době nedělá velké potíže, neboť Wireless LAN již dávno není v začátcích. Potíže s tvorbou bezdrátové domácí sítě mohou nastat pouze s příjmem, neboť bezdrátové sítě, stejně jako všechna zařízení využívající rádiových vln, zápasí čas od času s překážkami, které brání šíření signálu a tedy stává se, že daná domácnost se nachází v místě bez signálu a není možné tuto síť vytvořit.

Tato práce si z rozsáhlého námětu, jenž bychom mohli shrnout pod pojmem „bezdrátové sítě“, vybírá jen malý výsek. Výsek proto, protože v tomto rozsáhlém a dynamicky se rozvíjejícím prostředí komunikační technologie mezi počítači a nejen mezi nimi je v tak málo rozsáhlém pojednání nemožné zachytit vše dopodrobna. A dokonce i tento výsek se týká v teoretické části jen těch nejdůležitějších věcí které je třeba objasnit.

3. Cíl práce a metodika

Jak již bylo v úvodu řečeno, práce se zabývá pouze výsekem rozsáhlého tématu bezdrátových sítí. Soustřeďuje se především na návrh domácí počítačové sítě pro dva domácí počítače s připojením k síti Internet.

Jednoduchý popis zavedení a zprovoznění takovéto sítě je pojat jako uživatelská příručka pro běžného uživatele, který má pouze minimální znalosti o sítích a jeho počítačová gramotnost je na základní uživatelské úrovni. Pro takového uživatele by tato příručka měla představovat jednoduchý návod na realizaci domácí bezdrátové počítačové sítě.

V úvodu práce jsou shrnuty základní informace o bezdrátových počítačových sítích, o jejich rozdělení a jejich rozsahy, které používají. V samostatné kapitole je podrobněji rozebráno zabezpečení těchto sítí a jejich ochrana proti vnějším vetřelcům. V této kapitole jsou uvedeny také nové trendy v tomto oboru. Jsou zde zhodnoceny výsledky tohoto vývoje a nastíněn nastupující směr vývoje.

Těžištěm této práce je poslední kapitola, která obsahuje popis vytvoření bezdrátové sítě pro domácí využití s připojením k síti Internet formou uživatelské příručky pro běžného počítačového uživatele.

4. Úvod do bezdrátových sítí

Většina uživatelů si asi již kladla 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 druhou stranu bezdrátové sítě nabízejí podstatně nižší rychlosti než nejmodernější ethernetové kabelové sítě. Pokud uživatel nezamýšlí přenášet v síti velké objemy dat najednou, mohou snadno výhody bezdrátové sítě převážit.

[3] 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.

[3] Bezdrátové sítě **existují od roku 1992**, tehdejší zařízení ale pracovala na provozních rychlostech hluboko pod 1 Mbit/s. V té době také chyběl jakýkoliv standard, takže bylo nutno používat síťové prvky stejného výrobce. Tato situace se významně zlepšila po přijetí standardu **IEEE 802.11**, jímž jsou moderní WLAN sítě definovány a standardizovány.

4.1. Standard IEEE802.11b a WiFi

[2] Když se dnes hovoří o bezdrátových sítích, často se některé zkratky zaměňují.

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 řekne WLAN.

[2] Dalším termínem je **IEEE 802.11b nebo 802.11g**. Tento pojem představuje označení standardu standardizačního institutu IEEE - jde o standard definující bezdrátové sítě v nelicencovaném pásmu 2,4 GHz. Písmenko B na konci označuje standard pro maximální rychlost až 11 Mbit/s, zatímco novější standard G označuje maximální rychlosti až 54 Mbit/s. Na konci můžete najít i další písmenka - tím je zpravidla odlišena jiná verze standardu či skutečnost, že tento derivát standardu IEEE802.11 pracuje na jiné frekvenci (to v případě 802.11a). Přehled těchto derivátů je podrobně uveden dále.

[2] Další důležité označení je **WiFi - Wireless Fidelity**. Tato zkratka se často zaměňuje s označením IEEE802.11a/b/g. Jde totiž o označení a logo udělované výrobkům pracujícím podle standardu 802.11a/b/g, které jsou mezi sebou vzájemně propojitelné. Výrobky označené WiFi tedy můžete vcelku bez obav propojovat s jinými výrobky označenými logem WiFi od jiných výrobců – s tím omezením, že výrobky dle standardu 802.11a nelze propojit s výrobky 802.11b/g. To je ale zřídkavý případ, pokud se někde používá málo rozšířené a v Evropě nepovolené 802.11a, pracuje v duálním režimu i s 802.11b nebo g.

Značka WiFi není 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 výrobky různých výrobců 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 tohoto standardu, protože jde o zapamatovatelnější 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 zařízeních pracujících podle standardu. Tohoto dělení se budeme držet také.

4.1.1. Frekvenční rozsahy IEEE802.11

[1] Bezdrátové sítě standardu IEEE802.11 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. Kromě tohoto pásma se pro WiFi sítě vyhrazuje ještě pásmo 5GHz. To používá zatím technologie 802.11a, jenže v Evropě není vítána a tak se čeká na jejího nástupce označovaného jako 802.11h, jenž již evropským předpisům vyhovuje.

[1] Frekvenční rozsah se ovšem liší země od země - v některých státech není povolené plné frekvenční spektrum, protože jeho části jsou již využívány

pro jiné účely. Pro nás je příjemné, že ČTÚ povoluje 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 pro WiFi v pásmu 2,4 GHz		
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

4.1.2. Standard 802.11

[3] Standard 802.11 **vznikl v roce 1997** 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, utvářely se v rámci této pracovní skupiny další pracovní podskupiny věnované rozšířením a změnám v rámci tohoto standardu. 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 http://www.ieee.org/. Novější revize standardu zatím nebyla vydána a jsou pouze ve fázi rozpracování, diskuse nebo schvalování.

Dále jsou uvedeny jednotlivá rozšíření standartu IEEE 802.11:

802.11a - WLAN v pásmu 5 GHz a s rychlostí až 54 Mbit/s.

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

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

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

802.11d - Mezinárodní harmonizace. Se vznikem standardu 802.11 se ukázalo, že je potřeba mezinárodní kooperace a harmonizace. Zejména pásmo 5 GHz se používá v mnoha státech různě a bylo třeba tomu standardizaci přizpůsobit tak, aby nevycházela vstříc pouze potřebám USA a Japonska. To měla za úkol tato pracovní skupina.

802.11e – rozšíření Medium Access Kontrol (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) trvalý tok jeho dat měl přednost před přenosem dat uživatelů, kteří například jen stahují poštu a chvilkový výpadek naprosto nepoznají, zatímco v hlasu nebo videu by byl hodně poznat.

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

proprietárním řešením, nebo celou záležitost řešit úplně mimo přístupové body.

[2] 802.11g - "Higher Speed Physical Layer (PHY) Extension to IEEE 802.11b", je zpětně slučitelná s 802.11b (pracuje ve stejném pásmu 2,4 GHz), takže umožňuje rozšířit stávající infrastrukturu podnikových WLAN i veřejných přístupových sítí (hot spots). Na rozdíl od WiFi, které bylo schváleno už před čtyřmi lety a které za poslední dva roky zažilo velký rozvoj, je ale rychlejší. Maximální teoretická rychlost nejnovější normy se pohybuje do 54 Mbit/s (maximální kapacita 802.11b na fyzické vrstvě je 11 Mbit/s). Reálná kapacita se bude pohybovat do 30 Mbit/s, podobně jako u 802.11a (uživatelská datová rychlost u 802.11b dosahuje maximálně 6 Mbit/s). Zvýšená kapacita WLAN u 802.11g znamená rovněž možnost podporovat až pětinásobně více uživatelů.

Rychlostí bude tedy 802.11g konkurovat starší normě 802.11a, která se však ve světě zatím neujala tak jako pomalejší WiFi. 802.11a, ale na rozdíl od obou konkurenčních WLAN pracuje v jiném bezlicenčním kmitočtovém pásmu: 5 GHz. Toto pásmo je méně vytíženo a hrozí v něm méně rušení než v hojně využívaném pásmu 2,4 GHz, kde pracují také bezšňůrové telefony, zařízení Bluetooth (IEEE 802.15) nebo třeba mikrovlnné trouby.

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. Velmi důležité, schváleno v červnu 2004.

802.11j - práce na alokaci nových frekvenčních rozsahů pro multimediální služby bezdrátových sítí. Jde o vysoké frekvence a ještě chvíli potrvá, než se budou vyrábět 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.

802.11s - mesh standard pro samoorganizující se WiFi sítě.

Jak je vidět, v praxi se především užívá „b“ pro WiFi, s písmenkem „a“ pro WiFi v pásmu 5GHz a s písmenkem „g“ pro zvýšení rychlosti WiFi. Ostatní písmenka označují funkce potřebné hlavně pro firemní a složitější sítě.

Pokud by vás zajímalo, proč se novější standard označuje jako „802.11a“ zatímco starší je označen jako „b“, pak je vysvětlení prosté - standard 802.11a je ve skutečnosti starší, ale technicky byl náročnější na implementaci, takže výrobky s WiFi5 přicházejí na trh později, než ostatní WiFi technologie.

[2] IEEE začal také nedávno pracovat na rychlejší WLAN, která má podporovat **reálné datové rychlosti 108 Mbit/s**. Cílem projektu **802.11n**, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Enhancements for Higher Effective Throughput", je modifikovat stávající fyzickou a vrstvu a podvrstvu MAC (Media Access Control) tak, aby se na úrovni MAC docílilo propustnosti minimálně 100 Mbit/s. Jde tedy nejen

o zvýšení fyzické propustnosti sítě, ale také o zvýšení kapacity vnímané samotným uživatelem.

[2] Skupina High Throughput Task Group má za úkol řešit problémy současných specifikací, které ovlivňují reálnou přenosovou kapacitu, jako rušení a následné ztráty paketů. Opravy chyb při přenosu nebo šifrování/dešifrování jsou činnosti, které samy kladou značné nároky na přenosovou kapacitu a tak ji ubírají užitečnému uživatelskému provozu. Úkolem bude tuto režii snížit na minimum.

Využití rychlé WLAN se očekává jak v podnikových, tak v domácích sítích, a také ve veřejných přístupových bezdrátových sítích (hot spots). Nové produkty podle specifikace pod označením **802.11n** se začaly objevovat na trhu mají na trhu v roce 2005. Vývoji rychlosti WLAN se meze nekladou, požadovaných 100 Mbit/s je minimum, seriózně se hovoří dokonce o **320 Mbit/s**.

4.2. Organizace: IEEE

[4] IEEE (Institute of Electrical and Electronics Engineers) je mezinárodně uznaná organizace sdružující elektro-inženýry (v současnosti je jich kolem čtvrt milionu ze 150 zemí světa). Členství v IEEE je individuální, otevřené všem dobrovolníkům. Kromě vzdělávací a publikační činnosti vytváří IEEE důležité technické normy (IEEE Standards Association, IEEE-SA). Ve svém portfoliu má přes 870 schválených norem a přes 400 je ve vývoji. Asi nejznámější normy IEEE se týkají oblasti komunikačních sítí: výbor IEEE 802 normalizoval prakticky všechny lokální a metropolitní sítě (LAN a MAN), např. 802.3 (normalizovaný Ethernet), 802.5 (normalizovaný Token Ring). Výjimkou je

pouze FDDI (Fiber Distributed Data Interface) a Fibre Channel, které spadají do působnosti ANSI (American National Standards Institute).

Poznámka: Normy IEEE 802 jsou v současnosti volně k dispozici ke stažení (zpřístupněny po šesti měsících od schválení, dříve je možné je zakoupit v elektronické nebo tištěné podobě). Stav přípravy a publikování norem lze zjistit v celkové zprávě IEEE Standards Status Report nebo konkrétně vyhledat na adrese „http://standards.ieee.org/db/status/index.shtml“.

5. Bezpečnost WLAN

5.1. Zabezpečení WLAN

V červnu roku 2004 IEEE schválil normu pro doplňkové bezpečnostní mechanizmy bezdrátových lokálních sítí 802.11a/b/g. Tyto nové normy odstraňují problémy s WEP (Wired Equivalent Privacy), dochází tím k zlepšení autentizace i šifrování. Nyní je třeba podrobněji si ukázat poznatky nové normy její přínos a poukázat na problematiku přechodu na plné zabezpečení – tedy co je třeba upgradovat či vyměnit.

Bohužel se stává, že uživatelé jsou přes všechna upozornění, hojně publikovaná v tisku, stále neopatrní a nechtějí se pouštět do zdánlivě složité konfigurace WLAN pro zajištění vyšší úrovně zabezpečení. Často nezapnou ani protokol WEP (Wired Equivalent Privacy) a nechávají svou síť otevřenou, na pospas potenciálním vetřelcům. Stále ponechávají některá nastavení na implicitní hodnotě tak, jak byla nastavena při výrobě (např. SSID, Service Set IDentifier).

V takových případech může dojít k problémům: jejich síť může využívat někdo cizí a získat tak přístup ke službám, které si oběť platí (např. širokopásmový přístup k Internetu, k němuž je WLAN v podniku nebo doma připojena). Jejich data - uložená a přenášená - jsou v nebezpečí odposlechu, krádeže, případně modifikace. Dokonce samotní uživatelé a jejich identita může být ohrožena.

5.2. Nová norma

[4] Naštěstí během posledních dvou let se udělalo hodně práce na vybudování skutečně bezpečného technologického zabezpečení WLAN. Pokud vezmeme v úvahu normu IEEE 802.11i a jejích předpokládané prvky, kterými zajistí bezpečnou komunikaci v rámci WLAN, byl vývoj velice zdlouhavý. Její dokončování a zejména schvalování trvalo opravdu dlouho. 802.11i byla na zasedání RevCom IEEE schválena. Plné znění normy je následující:
IEEE 802.11i Amendment to Standard [for] Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements

[4] Pro zajímavost: kromě 802.11i byly schváleny ještě další tři normy, které na přijetí dlouho čekaly:

- IEEE 802.3ah Amendment to Standard [for] Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 3: Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications - Media Access Control Parameters, Physical Layers and Management Parameters for Subscriber Access Networks,
- IEEE 802.16 Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems,
- IEEE 802.17 Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan

Area Networks - Specific Requirements - Part 17: Resilient Packet Ring (RPR) Access Method & Physical Layer Specifications.

Mezi schválenými normami tedy ještě chybí druhá důležitá doplňková specifikace pro WLAN, podobně netrpělivě očekávaná jako 802.11i, tentokrát na podporu QoS (802.11e).

5.3. Od WPA k 802.11i

Uvedeme nyní jaké mechanizmy pro zabezpečení WLAN nová norma nabízí. Některé prvky budou zákonitě povědomé, protože je používá dočasné řešení pro zabezpečení (WPA, WiFi Protected Access), které před rokem a půl navrhla WiFi Alliance. WPA zahrnuje podmnožinu bezpečnostních mechanizmů navržených pro 802.11i, které nevyžadovaly víc než softwarový upgrade pro zařízení.

Nové bezpečnostní mechanizmy v rámci WPA musely odstranit zásadní nedostatky protokolu WEP, tedy prakticky nulovou autentizaci a velmi slabé šifrování statickým klíčem. Autentizace se zlepšila prostřednictvím použití obecného rámce řízení přístupu podle 802.1x (Port-Based Network Access Control), EAP (Extensible Authentication Protocol), nebo alternativně přednastaveného sdíleného klíče (PSK, PreShared Key). Pro šifrování se místo WEP použil nový protokol pro šifrování dynamickým klíčem, TKIP (Temporal Key Integrity Protocol), a zavedl se také management klíčů. Kromě toho se kontroluje integrita zpráv pomocí algoritmu přezdívaného Michael (MIC, Message Integrity Check).

To vše najdeme také v 802.11i, ale k protokolu TKIP, který může pracovat s minimálními požadavky na softwarový upgrade na stávajících zařízeních s hardwarem pro WEP, se přidal nový protokol CCMP (Counter-mode CBC (Cipher Block Chaining) MAC (Message Authentication Code) Protocol), zaručující silnější šifrování díky využití AES (Advanced Encryption Standard) právě v režimu CCM (kombinuje režim CTR, Counter Mode, pro utajení a CBC-MAC pro autentizaci a integritu). AES je považován za dostatečný šifrovací mechanizmus i pro vládní účely, na rozdíl od slabého mechanizmu RC4, který se používal v protokolech WEP i TKIP. Zatímco dříve stačilo útočníkovi odposlechnout dostatečný objem zpráv, aby mohl zlomit klíč WEP a jedinou obranou byla včasná manuální změna klíče, s 802.11i se mění šifrovací klíče automaticky. Jinak 802.11i podobně jako WPA nabízí dvojí režim pro autentizaci, PSK a 802.1x a autentizace probíhá oboustranně.

[1] 802.11i, ne náhodou nesoucí označení RSN (Robust Security Network), zcela nahrazuje WEP. Pro plně bezpečnou síť je ovšem nezbytný protokol CCMP, zatímco TKIP je volitelný. RSN ovšem není zadarmo: vyžaduje od bezdrátových zařízení takové schopnosti, které většina z nich dnes ještě nemá, zejména s ohledem na procesní možnosti pro silné šifrování.

[1] Jak jsou odolné všechny vývojové stupně bezpečnostních řešení, která jsou dnes k dispozici pro WLAN, vůči různým typům útoků na podnikové sítě, naznačuje následující tabulka:

	WEP	WPA	802.11i (WPA2)
autentizace	otevřená	EAP-TLS (EAP-Transport Layer Security) nebo PEAP (Protected EAP)	EAP-TLS nebo PEAP
šifrování	statický WEP	TKIP/CKIP (Cisco Key Integrity Protocol)	AES
útok:		**odolnost:**	
na integritu, důvěrnost dat, man in the modele	dobrá	lepší	nejlepší
falešná autentizace	slabá	nejlepší	nejlepší
na slabý klíč	slabá	nejlepší	nejlepší
falšované pakety	minimální	nejlepší	nejlepší
falešný přístupový bod	minimální	lepší	lepší
Úroveň šifrování	pro domácí síť (40- nebo 104bitový klíč; 24bitový vektor IV)	pro podnikovou síť (128bitový klíč; 48bitový vektor IV)	pro podniky i vládu (128+bitový klíč; 48bitový vektor IV)

Doporučení ohledně uplatnění WEP, WPA nebo WPA2 s ohledem na využití v různých typech sítí lze shrnout následovně:

	autentizace	**šifrování**	**použitelnost pro podnikové sítě**	**použitelnost pro domácí a malé sítě**
WEP	nulová	WEP	horší	dobrá
WPA (PSK)	PSK	TKIP	horší	nejlepší
WPA2 (PSK)	PSK	AES-CCMP	horší	nejlepší
WPA (plná)	802.1x	TKIP	lepší	dobrá
WPA2 (plná)	802.1x	AES-CCMP	nejlepší	dobrá

Z výše uvedeného je zřejmé, že ne vždy je nutné pro kvalitní zabezpečení použít WPA2. Pro domácí sítě, malé kanceláře a malé podniky např. postačí stávající WPA, protože pro ně WPA2 neznamená výrazný přínos, respektive nutnost.

5.3.1. Testování bezpečných produktů

Otevřené řešení je tedy hotové a nové produkty se mohly na jeho základě brzy začít testovat ve WiFi Alliance pod označením WPA2 (vycházely z 802.11i a specifikovaly povinnou "výbavu" zařízení pro zajištění bezpečnosti) pro

odlišení od původní WPA. Očekávalo se, že testování bude připraveno na září 2004. Podle předpokladů bylo WPA2 zpětně slučitelné s WPA.

Použití AES pro šifrování si však může vyžádat úpravy i v hardwaru kvůli náročnosti šifrování. Každý, kdo má instalovanou WLAN a chtěl by ji ještě lépe zabezpečit právě pomocí WPA2, by si měl u "svého" výrobce ověřit, jak bude možné takový upgrade provést (zda vůbec). Typicky přístupové body a koncová přenosná zařízení budou vyžadovat nový hardware. Některé produkty již mohou mít zabudovanou podporu pro šifrování podle AES, přesto však budou potřebovat upgrade softwaru nebo firmwaru pro plnou podporu 802.11i.

Firemní bezpečnostní řešení, kterých se za dobu neexistence normy objevilo dost, totiž mají pochopitelně problém se spoluprací se zařízeními jiných výrobců, protože jejich principy nejsou dostatečně veřejně známy. Otevřené řešení tak přináší - na základě certifikace (testování jednak slučitelnosti s normou a jednak vzájemné spolupráce s jinými zařízeními) - jistotu možné kombinace certifikovaných produktů v jedné síti a také nižší výrobní náklady na zařízení.

Žádné bezpečnostní řešení v síti však nemůže být stoprocentní. Ani nová norma 802.11i nezaručuje, že odolá všem budoucím útokům. Zařízení s WPA2 ale budou dostatečně dobře technicky vybavena pro dnešní bezpečnostní situace, s nimiž se zejména podnikové sítě potýkají. Nicméně technické možnosti zařízení nestačí, vždy bude na koncovém uživateli, aby se seznámil s bezpečnostními mechanizmy, porovnal je se svými potřebami a nakonfiguroval příslušnou podporu pro zvolené bezpečnostní řešení. Bezpečnost WLAN nebude ani s novou normou řešitelná pouhým důvěřivým přístupem plug’n’play.

5.4. Nové normy pro (W)LAN

V roce 2004 se zvýšil počet norem pro bezdrátové LAN (WLAN). Pod hlavičkou výboru IEEE 802, který je hlavním správcem a tvůrcem norem pro LAN, vzniklo také několik důležitých a veskrze zajímavých specifikací pro metropolitní sítě.

Další odstavec uvádí stručný přehled stávajících norem a projektů, které by měly v blízké budoucnosti vyústit v další, obohacující specifikace.

5.5. Nová zaměření bezdrátových technologií

Po roce 2004 přibyly nejen schválené normy a nové projekty, ale také celé nové podvýbory IEEE 802 (Institute of Electrical and Electronics Engineers), které se věnují bezdrátovým sítím:

- **IEEE 802.11** - bezdrátové lokální sítě (Wireless Local Area Network, WLAN);
- **IEEE 802.15** - bezdrátové osobní sítě (Wireless Personal Area Network, WPAN);
- **IEEE 802.16** - širokopásmový bezdrátový přístup (bezdrátové metropolitní sítě, Wireless Metropolitan Area Network, WMAN; v roce 2004 byla schválena komplexní norma 802.16, která se dříve označovala jako doplněk 802.11d a která se stala základem pro WiMAX, neboť zahrnuje původní doplněk 802.11a;
- **IEEE 802.20** – širokopásmové mobilní bezdrátové sítě (Mobile Broadband Wireless Acces, MBWA)
- **IEEE 802.21** - předávání uživatelů mezi sítěmi, a to nejen bezdrátovými (Media Independent Handoff);

- **IEEE 802.22** - bezdrátové regionální sítě (Wireless Regional Area Networks, WRAN).

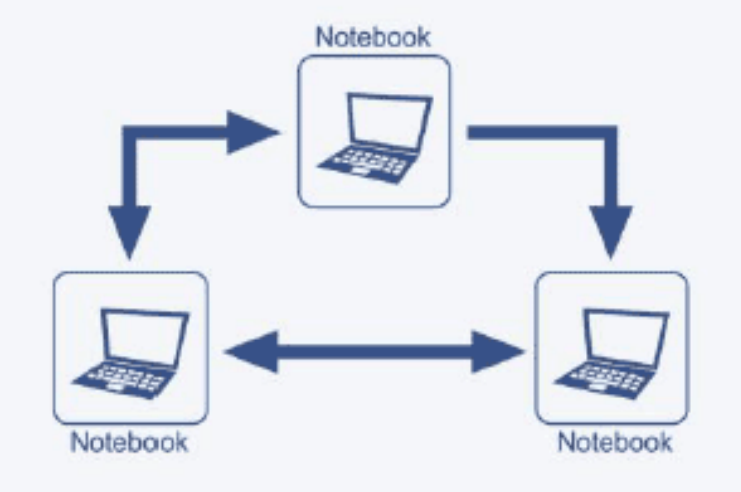
Podvýbory 20, 21 a 22 vznikly nedávno a zabývají se tématikou, která jde nad rámec stávajícího zaměření IEEE: MBWA doplňuje do pevného bezdrátového přístupu mobilitu (ta dosud nebyla prioritou), 802.21 řeší roaming pro mobilní/přenosná koncová zařízení mezi sítěmi různých typů. A konečně nejnovější 802.22 (Policies and Procedures for Operation in the TV Bands) se má zabývat využitím kmitočtového spektra dosud vyčleněného pro TV vysílání a jeho možným otevřením pro rychlé služby v regionálních bezdrátových sítích (WRAN), protože nižší kmitočty umožní delší dosah, a to i přes 40 km. Připravovaná norma bude doplňkem pro pevný metropolitní bezdrátový přístup (802.16), který není uzpůsoben pro využití TV spektra.

6. Návrh řešení WiFi sítě pro dva domácí počítače

6.1. Jak vytvořit malou bezdrátovou síť

Tato kapitola se zabývá popisem, jak instalovat a zprovoznit malou bezdrátovou síť.

Pokud je počítačů málo, bude 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 **[2]** 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 je třeba, 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.



Obrázek 1: propojení notebooků v síti ad-hoc.

Díky všem těmto omezením a hlavně díky jednoduchosti ad-hoc sítí je dále stručně uvedeno, jak se tyto sítě nastavují.

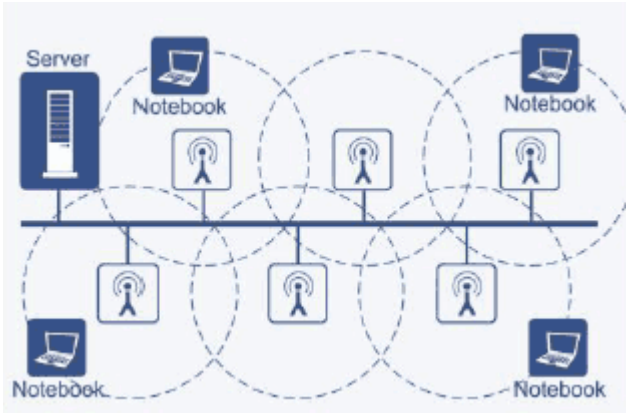
Schopnost práce v ad-hoc sítích musí být na většině zařízení aktivována v menu a protože se zařízení většinou připojují do sítí infrastrukturních (viz dále) a karta musí být zapnuta jen v jednom režimu, výrobci většinou nastavují infrastrukturní režim.

Pokud je WiFi technika přepnuta do režimu ad-hoc (novější karty se automaticky přepínají podle režimu, jakým disponuje protistrana), je třeba správně nastavit síť, tedy v nastavení TCP/IP nastavit IP adresy lišící se až v D segmentu, tedy tak, aby první tři čísla byla stejná, například 192.168.1.10 pro první kartu a 192.168.1.11 pro kartu druhou. Stejně tak je nutno nastavit shodný netmask, síťovou masku - například na 255.255.255.0. IP adresy shodné samozřejmě být nesmějí. Po tomto nastavení (a u starších Windows po restartu), pokud jsou oba počítače v "radiové dohledové vzdálenosti", měly by schopny spolu komunikovat.

6.1.1. Infrastrukturní sítě

[1] Protipólem sítí ad-hoc jsou sítě infrastrukturní, tedy sítě vybavené speciálním komunikačním prvkem zvaným access point, zkráceně AP, nebo APčko či spisovně přístupový bod. Díky němu jednotlivé počítače nemusí komunikovat 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.

[1] Následující obrázek znázorňuje již složitější síť, kde "páteř" tvoří pevně vedený ethernet, ten propojuje jednotlivé access pointy a teprve z nich se šíří signál WiFi sítě k notebookům. Do této sítě je možno zahrnout roaming, tedy možnost plynulého přechodu z jednoho access pointu k druhému bez nutnosti změny nastavení sítě.



Obrázek 2: případ sítě, kde notebooky jsou připojeny k serveru pomocí infrastrukturní sítě.

6.1.2. Co je to přístupový bod

Přístupový bod 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 ne každý access point zvládne velké množství najednou připojených uživatelů. Levnější access pointy mohou obsloužit jen kolem třiceti 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, je třeba koupit více access pointů. Z dále popsaného důvodu to bude výhodnější.

Je důležité si uvědomit, že **všichni klienti připojení na jeden AP sdílejí rychlostní pásmo 11 Mbit/s**, takže sto najednou připojených klientů musí vystačit s rychlostí 100 Kbit/s, kterou jim jednotlivě může přístupový bod ve sdíleném pásmu nabídnout. Už z toho důvodu AP nepodporují více jak 254 klientů. Některé access pointy ovšem umožňují "duální provoz". AP totiž v podstatě není nic jiného, než WiFi PCMCIA karta s přídavným hardwarem, který se stará o možnost upgrade a management karty, jakož i o routing dat do ethernetu. Prakticky lze AP velmi jednoduše udělat z jakékoliv WiFi karty, zatímco ceny WiFi karet jsou cenově velmi nízko tlačeny značnou konkurencí a snadností výroby, access pointy se prodávají poměrně draho a tak se výrobci z normálních WiFi karet snaží firmware pro fungování v režimu access point

odstranit. I toto lze obejít a udělat si vlastní access point - například pro Linux a určité čipové sady takováto utilita existuje pod názvem HostAP.

Trh výrobců je následující: 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 Mbit/s. Například access point Orinoco AP-2000 pracuje se dvěmi PCMCIA kartami, které navíc nejsou zahrnuty v jeho ceně. Na jednu stranu je nutné si je dokoupit, na stranu druhou, až po přechodu na WiFi5 nebo na rychlejší 802.11g standard, stačí dokoupit nové PCMCIA karty. Takový AP ovšem bývá už dost drahý a hodí se spíše pro potřeby firemních klientů.

Co se rychlostí týká, kromě staršího a dnes nejrozšířenějšího WiFi 802.11b, tedy sdílené rychlosti až 11 Mbit/s, jsou k dispozici i další rychlosti, většina z nich ale není standardizována a závisí na použité čipové sadě. Čipovou sadou se rozumí srdce každého WiFi zařízení, zbytek tvoří pouze rozhraní a obslužné programy. Na čipové sadě tedy je, jakou rychlost a jak dobře ji podporuje. Jednotlivé nestandardizované rychlosti lze tedy využívat většinou i mezi zařízeními jiných výrobců, pokud používají stejnou čipovou sadu.

802.11g nabízí sdílených 54 Mbit/s a je nejvyšší standardizovanou rychlostí pro WiFi.

B Plus nebo TurboB - rychlost 22 Mbit/s u některých čipových sad Atheros (nestandardizováno, málo používané) - starší výrobky D-Link.

Super G - Atheros technologie nabízející 108 Mbit/s (nestandardizováno), používá D-Link a Proxim.

Afterburner - technologie Broadcom nabízející 125 Mbit/s (nestandardizováno), používá Buffalo a Linksys.

Xtreme - čipová sada PRISM Nitro MX Xtreme Multimedia, rychlosti až 140 Mbit/s, označení Xtreme není pevné, sám výrobce PRISM firma Conexant žádné speciálně nepropaguje a nechává to na výrobcích zařízení. Nestandardizováno, používají SMC, GlobespanVirata a další.

Turbo nebo Turbo G - u výrobků s čipovou sadou TI TNETW1130+, rychlosti 100 Mbit/s. Nestandardizováno. TI sady používají Netgear, Samsung, Sitecom, SMC Networks, US Robotics, Alpha Networks, AMIT, AboCom Systems, ASUSTeK, Global Sun Tech, Mototech a další.

Další významný výrobce WiFi čipových sad, firma Intel, nenabízí žádnou proprietární technologii pro zvýšení rychlosti a drží se standardů. Spolupráci mezi rozdílnými značkami, byť osazenými stejnou čipovou sadou, je lépe vyzkoušet předem.

Pokud výrobky neumí stejnou proprietární rychlost, pracují na nejbližší společné standardizované rychlosti, tedy podle standardu 802.11g nebo 802.11b. Rychlost udává nejpomalejší prvek sítě.

Správný access point by měl umět pracovat s DHCP servery tak, že do sítě řízené DHCP serverem ho jen připojíte a on si sám nakonfiguruje své připojení

do sítě. Kromě DHCP klienta také AP většinou obsahuje DHCP server, takže automaticky přiděluje adresy bezdrátovým klientům.

6.1.3. Access point

[1] Některé umožňují pracovat na více kanálech najednou, tedy vlastně umožní násobit pásmo 11 Mbit/s. 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 AP určená hlavně pro domácí použití. Problém ale není ani tak v tom, že nelze připojit více uživatelů najednou - to u domácích sítí nehrozí, protože se jedná o propojení několika počítačů. Horší je nízká odolnost proti DOS útokům, tedy pokusům o zahlcení takového access pointu síťovými dotazy - pomalý procesor se s tím obtížně vyrovnává. Pro malou domácí síť ale, není levný AP úplně špatnou volbou.

[1] WiFi zařízení se v principu musí řídit jednotným standardem, takže další odlišnosti jsou spíše v možnostech, které AP 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 lze požadovat např. povolovat či zakazovat přístup uživatelů rozpoznaných podle MAC adresy, limitovat jim vyhrazenou přenosovou kapacitu, AP může mít i svůj firewall a další. Čím více a čím podrobněji a jednodušeji lze takové parametry nastavovat, tím vyšší je potenciální cena AP. Nepřekvapí tedy, že výborný 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 zejména pro menší uživatele,

naopak na opačném konci jsou méně známé výrobky jako Zcomax (Z-Com), iTec, Benq a další podobné.

Tím ale nelze říci, že takové "no-name" výrobky jsou naprosto nepoužitelné. Právě naopak – pro technicky založené uživatele je výhodou, 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 si s ním vystačí, ačkoliv například management iTec zařízení je oproti jen o málo dražšímu D-Linku velmi obtížný.

Dnes už je docela běžné, že AP lze upgradovat tak, že se ze stránek výrobce stáhne soubor s novým firmware a nahraje se do APčka. 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 novou funkci doplní.

6.1.4. WDS

Důležitým prvkem (WDS) pro výstavbu trochu náročnější bezdrátové sítě může být systém WDS. Jde o proprietární, ale dnes velmi rozšířené řešení pro předávání signálu od jednoho přístupového bodu na druhý. Přístupové body se při použití WDS nemusí propojovat do Internetu ethernetem, ale propojují se mezi sebou bezdrátovou sítí. Vypadá to úžasně, má to ale i své technické limity, protože propojení používá stejný kanál, jako propojení s klientem, takže rychlost velmi klesá. Málokdy lze propojit více jak šest či osm zařízení přes WDS - přesto

je to velmi užitečná funkce a je vhodné jí věnovat při výběru přístupového bodu nebo směrovače pozornost.

6.2. Bezpečnost - WEP nebo WPA

Posledním podstatným rozdílem mezi jednotlivými přístupovými body (a obecně jakoukoliv WiFi technikou) je podporované zabezpečení. Starší bezpečností standard WEP nepatří mezi dokonalé a pro sítě s požadovaným lepším zabezpečením je lépe se mu vyhnout a implementovat pouze výrobky, které využívají WPA. To bezpečnosti nabízí již podstatně více a navíc většinu výrobků s WPA by mělo být možné upgradovat na nejnovější schválený bezpečnostní standard 802.11i. Ten nabídne mimo jiné dynamickou výměnu klíčů a bezpečnost tím podstatně zlepší. Pro základní orientaci v bezpečnosti tedy stačí si pamatovat, že WPA je lepší, než WEP.

[2] Na závěr, se **zmíníme o home routerech** nebo též **broadband routerech - domácích nebo širokopásmových směrovačích**. Tato zařízení v podstatě kombinují směrovač určený pro směřování provozu do Internetu s access pointem. U těchto zařízení je zkušenost výrobce ještě důležitější, než v případě access pointu, protože možnosti nastavení a pohodlí při nastavování je zde pro nezkušeného zákazníka velmi důležité. Domácí směrovače jsou velmi populární pro sdílení pevného připojení (ADSL, kabelový modem) mezi více počítači, zpravidla obsahují čtyři ethernetová rozhraní a ve své bezdrátové verzi i rozhraní WiFi.

6.3. Vytvoření mini wifi sítě

Mini wifi síť připadá v úvahu, pokud máte například nějakým způsobem zajištěný přístup k internetu (ADSL, kabelovka, wifi) pomocí ethernetového kabelu připojeného k nějakému zařízení (ADSL modem, kabelový modem, wifi router). Chcete tuto internetovou konektivitu mít k dispozici „ve vzduchu“ po celém Vašem sídle. Anebo vůbec internetovou konektivitu nemáte, ale chcete si propojit své počítače umístěné po domě mezi s sebou.

To jak komplikovaný wifi router budete potřebovat se v tomto případě odvíjí od toho, co umí vaše zařízení připojující vás k internetu a co od nového wifi routeru všechno budete požadovat.

První otázkou je, zda vaše zařízení připojující vás k internetu disponuje NATem. Většinou je to tak, že kabelové modemy ho nemají, ADSL modemy někdy ano a někdy ne, wifi routery velmi často ano. Dá se to zjistit dotazem na toho, kdo vám zařízení dodal anebo pokusem - připojte k vašemu zařízení přes ethernetové kabely dva počítače najednou (pokud má dost LAN zdířek je to jednoduché a výsledek vašeho pokusu bude z vysokou pravděpodobností pozitivní, pokud nemá dost LAN zdířek, lze použít hub/switch).

Jestliže takto připojené počítače budou moci současně přistupovat k internetu, tak vaše zařízení NATem pravděpodobně disponuje. V takovém případě váš nový wifi router nemusí být vlastně “router”, ale obyčejné AP za cca 1000 Kč. Jediný jeho úkol je převádět signál skrytý v drátech na bezdrátový. Jediné, co v něm zřejmě půjde nastavovat bude zabezpečení wifi (WEP, WPA, MAC filter).

Pokud vaše zařízení připojující vás k internetu NATem nedisponuje, vyberte si wifi router, který ho má. Bude o něco dražší, ale většinou na něm naleznete více funkcí a také více LAN zdířek, takže si budete moci připojit i více počítačů kabely.

Váš další výběr zařízení se bude řídit podle toho, zda požadujete nějaké pokročilé funkce wifi routerů (sdílení tiskárny, kamery, USB disku, DynDNS apod.).

6.4. Propojení dvou lokálních sítí (LAN) mezi sebou (bridge)

Další případ popisuje situaci, kdy máte dvě sítě, které samy o sobě existují kousek od sebe a nejsou spolu propojeny, což je přesně to, co byste chtěli. Volíte zařízení, která dokáží tyto oddělené sítě přemostit. Pokud neuděláte chybu, tak po takovém spoji bude směřovat pouze provoz mezi těmito sítěmi. Nemusíte se tedy obávat toho, že si pomalejším wifi zpomalíte dvě rychlé sítě. Existují speciální zařízení pokrývající tento případ. Jsou jednoúčelová a protože v domácím nasazení nepříliš častá, tak i poměrně drahá. Musíte koupit dvě stejného druhu (jedno do každé sítě).

Druhá možnost je řešit pomocí obvyklých wifi routerů, třeba AP na jednu stranu a klientský router na druhou. Problém je, že ač mnoho zařízení takto zkonfigurovat jde, tak to není jejich obvyklý stav a není tedy v manuálu popsaný.

Důležitou otázkou (která ovlivní konfiguraci takového spoje) je, zda chcete mít sítě opravdu plně spojené (skoro jakoby mezi nimi byl kabel a byly sítí jedinou) anebo zda si chcete určovat, co přesně se mezi nimi má přenášet

(pokud např. je vaše jen jedna síť). Pak se mezi nimi objeví zase NAT nebo lépe pouze firewall.

6.5. Rozšíření pokrytí stávající sítě

Stane se, že jedno AP nepokryje celou lokalitu, kde signál chcete mít. Wifi pracuje s velmi malým výkonem a standardně s velmi špatnými anténami. V indoorovém nasazení výměna antén není možné. Pak lze přidat další AP do míst, kde signál není. Variant je několik.

Ve wifi je k tomuto určen režim WDS. Paradoxně je to řešení velmi špatné. Musíte totiž zařízení umístit tak, aby se jejich signály vzájemně překrývaly (aby jedno získalo konektivitu od druhého). Tak jich spotřebujete hodně. Navíc provoz v této síti se dubluje (od vás k nejbližšímu AP a pak po WDS lincích mezi AP), takže propustnost rapidně klesá.

Mnohem lepší postup je nasadit několik AP a páteřní linky mezi nimi vytvořit pomocí kabelů. První AP musí splňovat podmínky některého z výše uvedených scénářů (to je to první, které jste si pořídili) - NAT, DHCP apod. Další už mohou být levná. Připojujete k zdířkám LAN prvního. NAT i DHCP zajišťuje první AP.

Je potřeba pochopit, jak bude vše fungovat. Síť je jen jedna. Rozprostírá se přes všechna AP. Ale AP je několik a počítače to tak budou vnímat. První, co nebude fungovat je, že počítač se kterým budete pohybovat, si nebude vybírat AP s nejsilnějším signálem. K přechodu na jiné AP ho donutí až ztráta signálu k původnímu AP. Navíc se to neobejde bez výpadku spojení. IP se vám

pravděpodobně nezmění, ale stahování v IE třeba spadne. Je vhodné všem AP nastavit stejné SSID a zabezpečení. Nebudete muset počítač nastavovat tak pro každé AP zvlášť. Nesmí být ale nastaven stejný kanál, navzájem by se rušila.

6.6. Stavba domácí bezdrátové LAN

Na závěr se pokusíme provést konečné shrnutí našich poznatků z tohoto oboru formou rychlokurzu stavby domácí počítačové sítě pomocí bezdrátového LAN. V následujících deseti krocích si ukážeme stavbu takovéto sítě.

6.6.1. Krok 1 – Jak jednoduše nakoupit

Pro samotné bezdrátové zasíťování je třeba několika zařízení WLAN, fungující dle standartu IEEE 802.11b.

6.6.2. Krok 2 – Kam se základní stanicí (routerem)

Velmi důležitým krokem je výběr vhodného místa pro umístění přístupového bodu , který zajišťuje přenos rádiového signálu.

Router WLAN je zpravidla umístěn v blízkosti telefonní přípojky, neboť je často na stejném místě namontován i modem DSL. Přičemž by mělo být samozřejmě dodrženo aby se router nacházel v obytné části domu nikoli ve sklepních prostorách, aby byla vzdálenost k přístupovým bodům co nejmenší.

Dostupnost a síla signálu je závislá především na podmínkách v daném místě. Špatný signál je opravdu zřídka zaviněn nevhodným nebo poškozeným hardwarem. Častěji za to můžou tlusté zdi, železobeton a velké vzdálenosti. To,

jestli vaše bezdrátová síť bude fungovat dobře či špatně, je dáno spíše specifiky stavby než umístěním Access Pointu.

Umístěte tedy Vaše zařízení vedle modemu DSL nebo kabelového modemu a propojte jej pomocí síťového kabelu s modemem.

6.6.3. Krok 3 – Připojení

A je na čase připojit síťový kabel. Na routeru začne svítit několik diod. Vedle diody signalizující zapnutí zařízení je umístěna dioda připojení na Internet. Tato dioda svítí, když je připojení k Internetu aktivní. Symbol antény signalizující bezdrátovou síť v běžném provozu svítí, při aktivitě bliká. Pod čísly 1 až 4 se skrývají běžné konektory pro kabelovou LAN, kterými je každý router WLAN vybaven.

Router je nyní zprovozněn. Nyní je čas spojit se s ním. Nejprve však musíte nastavit přístup pomocí adaptéru WLAN.

6.6.4. Krok 4 – Nastavení bezdrátové karty pro PC

Před tím, než vložíte kartu do počítače nebo připojíte adaptér WLAN, se podívejte do návodu k vašemu zařízení! U mnoha zařízení WLAN je nejprve nutné nainstalovat software a poté hardware, jinak by mohlo dojít k problémům s rozpoznáním nainstalované karty.

Vložte nejprve do mechaniky CD s ovladači a nainstalujte je. Mimo nich se nainstaluje doplňkový software, který vám pomůže s připojením k Wireless Access Point nebo Wireless Router v dalším kroku.

Nyní vložte adaptér WLAN do slotu pro PC Card, připojte jej pomocí kabelu USB nebo nainstalujte do sběrnice PCI. Operační systém by měl kartu bez problémů rozpoznat a nainstalovat příslušné ovladače. Dále by se měl v pozadí spustit software WLAN, eventuálně mohou být nalezeny dostupné sítě WLAN.

6.6.5. Krok 5 – Spojení s routerem

Wireless router je již spuštěn. Nyní se pokuste navázat komunikaci. S tím vám pomůže software WLAN, který byl nainstalován spolu s ovladači adaptéru Wireless LAN.

Klepněte na ikonu softwaru WLAN (většinou to bývá ikonka představující symbol s anténou). Otevře se vám okno programu. Na záložce *Network Search*, popř. *Wireless Network* nebo *Bezdrátové sítě* a můžete nechat vyhledat dostupné bezdrátové sítě.

Router byl nalezen. Poklepáním se k němu můžete připojit. Software nyní hlásí, že jste se k routeru připojili. Všechny routery přidělují síťové adresy automaticky pomocí zabudovaného serveru DHCP.

6.6.6. Krok 6 – První test sítě

Windows stále nabízí relikt operačního systému MS-DOS – příkazový řádek. S jeho pomocí můžete připojení k bezdrátové síti otestovat. Spustíte jej: *Start/Spustit* a do vstupního pole napište *command* (Windows 9x a ME) nebo *cmd* (Windows 2000 a XP).

Nyní napište: *ping xxx.xxx.xxx.x. (číslo automaticky přiřazené síťové adresy)* a stiskněte enter. Tento příkaz pošle zprávu zařízení se síťovou adresou vašeho Wireless Router a čeká na odpověď. Dostali jste odpověď? Ano. Pak to znamená, že přístupový bod odpověděl a vy jste se úspěšně připojili k síti. Gratuluji.

6.6.7. Krok 7 – Nastavení routeru Wireless LAN

Nyní musíte nastavit router a Wireless LAN. Wireless Router je vlastně další síťové zařízení a taky se tak chová, proto k němu můžete bez problémů přistupovat. Každý router má nainstalovaný malý webový server, který umožňuje jednoduchou konfiguraci.

Jak je na Internetu běžné, k určitému webovému serveru se dostanete pomocí adresy. Tato adresa odpovídá právě používanému číslu (IP adrese routeru). Otevřete tedy váš webový prohlížeč a do adresního řádku vložte: http:// *xxx.xxx.xxx.x. (IP – adresa routeru)* a stiskněte Enter. Otevře se vám dialog s dotazem na uživatelské jméno a heslo. Tímto způsobem je váš router chráněn před neoprávněným přístupem. Standardní uživatelské jméno a heslo naleznete v návodu k routeru.

Dále zde všem doporučím, aby se řídili pokyny v návodu na používání routeru. V příručce kterou dostanete jako součást balíčku k vašemu WLAN zařízení. Dle tohoto podrobného návodu se vám podaří projít úskalím nastavení vašeho routeru. Neméně tak vás provede tento návod při aktivaci zabezpečení WEP.

6.6.8. Krok 8 – Bezdrátově na Internet

Nyní se již můžete těšit na večer plný bezdrátového surfování po Internetu. Předtím však ještě musíte routeru sdělit vaše přístupové údaje, které jste obdrželi od svého poskytovatele Internetu. Jsou to stejná data, která jste používali na vašem počítači.

Otevřete ve vašem internetovém prohlížeči konfigurační menu routeru. Popis jak na to je ve vašem návodu k routeru. Musíte zde najít záložku či bod *„Základní nastavení“ (Basic Settings)*, kam můžete vložit přístupové údaje.

Před tím, než menu opustíte, potvrďte nastavení klepnutím na tlačítko *Apply*, resp. OK. Wireless Router se nyní restartuje a připojí se k Internetu. Dioda připojení k Internetu signalizuje úspěšné připojení.

6.6.9. Krok 9 – Jste tam!

Zdá se, že se vám povedlo připojit k Internetu. Otestujte však i v tomto kroku úspěšnost připojení k síti. Spusťte opět příkaz ping, jak bylo popsáno v kroku 6, zadejte však název jiného počítače. Například zadejte formou: *ping seznam.cz* a stiskněte Enter.

Pokud v po zadání tohoto příkazu vloženého do příkazového řádku obdržíte odpověď, pak se vám podařilo připojení k rozsáhlé síti Internet. Mělo by tudíž fungovat také surfování po Internet.

7. Závěr

Závěrem tedy zhodnoťme toto pojednání. Tato práce měla za úkol představit bezdrátové sítě a jejich využití pro domácí počítačovou síť. Rozvoj tohoto typu sítí je v dnešní době velmi dynamický. Neustále se hledají a vytvářejí nové možnosti využití této technologie v rovině domácích sítí.

V dnešní době je síť Internet v domácnostech naprosto běžnou záležitostí a jeden počítač je také již minulostí a proto vzniká skoro nutnost vytvářet rozsahem malé sítě pro domácí využití. Pro sjednocení informačních technologií v domácnosti a jejich co nejefektivnější využívání.

Nejprve bylo nutno vysvětlit základní terminologii potřebnou pro další zpracování tohoto tématu. Především ukázka rozdělení základního standartu 802.11 a jeho podskupiny utvořené organizací IEEE a jejich další vývoj.

Další důležitou kapitolou je zabezpečení takovéto bezdrátové sítě. Vysvětlení základních principů ochrany sítě a také poukázání na nově vznikající možnosti zabezpečení domácí počítačové sítě proti útokům ze sítě Internet. Vysvětlení těchto metod a jejich využití v praktické sféře. Myslím že toto téma je stále dneska zanedbáváno především ze strany běžného uživatele, který mnohdy zapomíná jakoukoliv ochranu své sítě a umožňují tím případným hackerům aby se dostávali k jejich soukromým datům a také aby měli možnost odposlechu.

V další kapitole je postupně vysvětlováno v obecné úrovni jak vytvořit malou bezdrátovou síť toto je nejdůležitější část práce kde je pro běžného uživatele připraveno vysvětlení jak se v této problematice co možná nejsprávněji

zorientovat. Je zde vysvětlení základních bodů co je třeba vědět při vytváření takovéto sítě a jaké komponenty uživatel potřebuje aby si mohl tuto síť sám vytvořit na závěr je souhrn několika kroků pro úspěšné zapojení a zprovoznění takovéto sítě.

Tato práce by měla běžnému uživateli poskytnout alespoň minimální přehled a této problematice a dát mu základní znalost stavby počítačové sítě.

8. Seznam literatury

[1] Zandl, P. Bezdrátové sítě Wi-Fi – Praktický průvodce. Brno: Computer Press, 2003. ISBN 80-7226-632-2.

[2] Brisbin, S. Wi-fi. Praha: Neocortex, 2003. ISBN 80-86330-13-3.

[3] Shinder, D.L. Počítačové sítě. Praha: SoftPress, 2003. ISBN-80-86497-55-0.

[4] http://standards.ieee.org

9. Přílohy