VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT

INSTITUTE OF INFORMATICS

PROBLEMATIKA BEZDRÁTOVÝCH SÍTÍ

WIRELESS NETWORK

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — PETER ĎURAJ

AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. MILOŠ KOCH, CSc.

SUPERVISOR

BRNO 2011

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2010/2011
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Peter Ďuraj

Manažerská informatika (6209R021)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává bakalářskou práci s názvem:

Problematika bezdrátových sítí

v anglickém jazyce:

Wireless Network

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současné situace
Vlastní návrhy řešení, přínos návrhů řešení
Závěr
Seznam použité
literatury Přílohy

Seznam odborné literatury:

BARKEN,Lee. Wi-Fi: jak zabezpečit bezdrátovou síť. 1.vyd. Brno: Computer Press, 2004. 174 s. ISBN 80-251-0346-3.
BRISBIN, Shelly. Wi-fi: postavte si svou vlastní wi-fi síť. 1.vyd. Praha: Neocortex, 2003. 248 s. ISBN 80-86330-13-3.
KöHRE,Thomas. Stavíme si bezdrátovou síť Wi-fi. 1.vyd. Brno: Computer Press, 2004. 296 s. ISBN 80-251-0391-9.
ZANDL,Patrick. Bezdrátové sítě WiFi : praktický průvodce. 1.vyd. Brno:Computer Press, 2003. 190 s. ISBN 80-7226-632-2.

Vedoucí bakalářské práce: doc. Ing. Miloš Koch, CSc.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2010/2011.

L.S.

_____	_____
Ing. Jiří Kříž, Ph.D.	doc. RNDr. Anna Putnová, Ph.D., MBA
Ředitel ústavu	Děkan fakulty

V Brně, dne 21.05.2011

Abstrakt

Hlavným obsahom mojej bakalárskej práce bude uviesť problematiku bezdrôtových sieti. Vysvetľuje aktuálne používané štandardy a architektúry v bezdrôtových sieťach a ich bezpečnosť. V ďalšej časti nadväzuje analýza problému súčasnej situácie. Praktickou častou bude návrh súkromnej bezdrôtovej siete v ktorej treba dbať najmä na vysokú bezpečnosť.

Abstract

The subject of my bachelor thesis is the issues of wireless networks. It analyzes current standards and architectures used in wireless networking and its security. Next part focuses on present situation. The practical part contains projecting a wireless network specialized in high security.

Kľúčové slová

IEEE 802.11, WiFi, Prístupový bod, WEP, WPA, WPA2, RADIUS, Autentizácia, MAC adresa, Bezdrôtová sieť, Bezpečnosť

Keywords

IEEE 802.11, WiFi, Access point, WEP, WPA, WPA2, RADIUS, Authentication, MAC address, Wireless network, Security

Bibliografická citácia

ĎURAJ, P. *Problematika bezdrôtových sietí*. Brno : Vysoké učení technické v Brně, Fakulta podnikatelská, 2011. 59 s. Vedúci bakalárskej práce doc. Ing. Miloš Koch, CSc.

Čestné prehlásenie

Prehlasujem, že táto práca je mojim pôvodným autorským dielom, ktoré som vypracoval samostatne. Všetky zdroje, pramene a literatúru, ktoré som pri vypracovaní používal alebo z nich čerpal, v práci riadne citujem s uvedením úplného odkazu na príslušný zdroj (v zmysle Zákona č. 121/2000 Zb., o práve autorskom a o právach súvisiacich s právom autorským).

V Brne dňa 21.05. 2011

Peter Ďuraj

Poďakovanie

Týmto by som sa rád poďakoval pánovi doc. Ing. Milošovi Kochovi, CSc., vedúcemu mojej bakalárskej práce, za jeho prínosné rady a obzvlášť užitočnú pomoc, ktoré mi výrazne pomohli pri spracovaní tejto bakalárskej práce.

Obsah

Úvod

V súčasnosti sú bezdrôtové siete stále viac a viac používané a bezdrôtové pripojenie sa pomaly vyskytuje už skoro v každom podniku či domácnosti. Tieto bezdrôtové siete prinášajú veľa výhod v mnohých hľadiskách oproti káblovým sieťam a stále sa viac dostávajú na výslnie a ich priazeň vzrastá aj vďaka ľahkej implementácii na počítače. Uvedenie takejto siete do domácnosti alebo do firemných kruhov mnohonásobne zefektívni a zvýši ľahkosť pripojenia osôb či návštevníkov do siete a umožní im voľné a bezproblémové pripojenie k sieti. Dôležitý prínos má taktiež pri zväčšovaní, pretože uľahčuje prácu a šetrí finančné prostriedky oproti rozširovaniu klasickej LAN káblovej siete.

Bezdrôtové siete a ich používanie však so sebou prinašjú určité riziká a hrozby. Signál teda môže zachytiť cudzia osoba ale taktiež aj útočníci, ktorý sa prostredníctvom rôznych spôsobov a nástrojov môžu dostať k cenným dokumentom, ktoré môžu zmazať poprípade ľahko zneužiť. Tým pádom je dôležité sa dôkladne zaoberať vhodným zabezpečením bezdrôtovej siete hlavne keď sa v nej vyskytujú cenné priam nevyčísliteľné informácie.

Návrh siete budem robiť pre „Centrum voľného času deti a mládeže“. Toto centrum navštevuje mnoho detí, teda bezdrôtová sieť je v tomto prípade je skutočne potrebná.

Túto tému som si vybral, pretože je v súčasnosti veľmi skloňovaná v oblasti IT/IS a o tento sektor sa zaujímam, budem sa ju snažiť podať výstižne a odborne.

1 Cieľ práce

- Postupne popísať teoretické východiská a odborné výrazy v oblasti bezdrôtových sietí respektíve WiFi sietí;
- Vysvetliť a definovať problematiku ohľadom dôkladného zabezpečenia a zdôrazniť klady a zápory v tejto sfére;
- Analyzovať problémy súčasnej situácie;
- Predložiť návrh na vybudovanie funkčnej bezdrôtovej siete s dôrazom na bezpečnosť;
- Uviesť samotnú bezdrôtovú sieť a poukázať na možné hrozby útokov, ktoré môžu sieť ohrozovať z vonku.

2 Teoretické východiská práce

2.1 Čo je to bezdrôtová sieť

Pojem bezdrôtová sieť znamená a vzťahuje sa na akýkoľvek typ počítačovej siete, ktorá je bezdrôtová a je často spojená s nejakou telekomunikačnou sieťou, v ktorej je pripojenie vykonané bez akéhokoľvek použitia rôznych drôtov. Bezdrôtové siete vo všeobecnosti vykonávajú diaľkový prenos, ktorý pracuje na báze elektromagnetických vĺn, ako sú napríklad rádiové vlny, digitálne televízne vysielanie, mobilná komunikácia GSM, bluetooth a mnoho ďalších technológií.

2.2 Doby pred štandardom 802.11

V časoch pred zavedením štandardu 802.11 sa bezdrôtové dátové prenosy využívali iba pre špeciálne účely. Pretože chýbali štandardy vznikali rady pomalých protokolov a drahých zariadení, ktoré neboli vzájomne kompatibilné. (1)

Najobľúbenejšie bezdrôtové aplikácie z tých dôb boli bezdrôtové pokladne. Na ktorých bolo postupne možné prijímať platby kartou. Bezdrôtové spracovanie platobných kariet bolo možné integrovať do existujúcich účtovných procesov. Pričom on-line povaha transakcie minimalizovala rizika zneužitia kariet a uľahčovala účtovné spracovanie. (1)

Bezpečnosť týchto systémov bola typicky iluzórna. Bez znalostí použitých protokolov bolo zneužitie značne zložité. Väčšina spoločností spoliehala na „security by obscurity“ a bezpečnosť zaisťovala len prisním utajením technických podrobností použitého riešenia. (1)

2.3 Schválenie štandardu 802.11

Tento štandard bol prijatý v roku 1997 pod pôvodnou špecifikáciou 802.11. Spomínaný štandard podporoval prenosové rýchlosti 1 a 2 Mbit/s. Využíval frekvenčné pásmo od 2,4 do 2,4835 GH. Protokol pokrýval prvú fyzickú a druhú linkovú vrstvu OSI modelu. (1)

2.3.1 IEEE 802.11b

Rozšírenie základnej normy prišlo v roku 1999. Protokol je špecifikovaný pre pásmo 2,4 GHz, poskytuje však vyššie rýchlosti a to až 11 Mbit/s. Na ich dosiahnutie využíva nový spôsob kódovania, tzv. doplnkové kódové kľúčovanie (Complementary Code Keying, CCK) v rámci DSSS na fyzickej vrstve. Kódovanie CCK je istým variantom technológie CDMA, známej z moderných bezdrôtových sietí. (8)

Norma špecifikuje, že podľa momentálnej rušivosti prostredia sa dynamicky mení rýchlosť na nižšiu, alebo naopak na vyššiu: 11 Mbit/s, 5,5 Mbit/s, 2 Mbit/s, 1 Mbit/s. (Adaptívna selekcia rýchlosti) v prípade zhoršenej kvality signálu. (8)

Pásmo vyhradené pre bezlicenčné prenosy rozdeľuje na 11 pracovných kanálov (5 MHz pre každý) na nasledovné frekvencie:

- Kanál 1 – 2,412 MHz;
- Kanál 2 – 2,417 MHz;
- Kanál 3 – 2,422 MHz;
- Kanál 4 – 2,427 MHz;
- Kanál 5 – 2,432 MHz;
- Kanál 6 – 2,437 MHz;
- Kanál 7 – 2,442 MHz;
- Kanál 8 – 2,447 MHz;
- Kanál 9 – 2,452 MHz;
- Kanál 10 – 2,457 MHz;
- Kanál 11 – 2,462 MHz. (8)

Maximálna rýchlosť na fyzickej vrstve je síce už spomínaných 11 Mbit/s, ale použiteľná rýchlosť je nižšia, pretože 30-40 % teoretickej kapacity tvorí réžia. Testovaná užívateľná rýchlosť sa udáva okolo 6 Mbit/s pri použití TCP paketov, pre UDP pakety potom cca 7 Mbit/s. Dosah siete je vnútri budov 30 m v závislosti od množstva, hrúbky a materiálu priečok, okolo 100 m v exteriéri, a za vhodných podmienok je možné túto vzdialenosť aj mnohonásobne presiahnuť. Pri použití kvalitných smerových antén v nezarušenom priestore je možné dosiahnuť prenos aj na vzdialenosť desiatok kilometrov, ojedinele boli za vynikajúcich atmosférických podmienok zaznamenané prenosy na vzdialenosť vyše 100 km. (8)

Existujú rozšírenia 802.11b na rýchlosti 22, 33 a 44 Mbit/s ale neboli zakotvené v IEEE štandarde. Nazývajú sa aj 802.11b+. Tieto rozšírenia boli odstránené vývojom 802.11g, ktorý definuje prenosové rýchlosti až do 54 Mbit/s a je spätne kompatibilný s 802.11b. (8)

2.3.2 IEEE 802.11g

V roku 2003 štandard prináša ďalšie zvýšenie prenosovej rýchlosti. Hlavným prínosom novej špecifikácie je rozšírenie komunikačnej rýchlosti na teoretické maximum 54Mbit/s pri zachovaní spätnej kompatibility s 802.11b. (8)

Zvýšenie rýchlosti je dosiahnuté použitím nových modulačných techník orthogonal frequency-division multiplexing (OFDM). Nový štandard teda dokáže prepínať nielen medzi rýchlosťami, ale prepína aj modulačné techniky:

- Pre rýchlosti 6, 9, 12, 18, 24, 36, 48 a 54 Mbit/s používa OFDM
- Pre rýchlosti 5,5 a 11 Mbit/s používa CCK nad DSSS
- Pre rýchlosti 1 a 2 Mbit/s prepína do režimu DBPSK/DQPSK+DSSS (8)

2.3.3 IEEE 802.11a

Súbežne s prácami na štandarde IEEE 802.11b boli rozbehnuté práce aj na štandarde 802.11a, ktorý bol uvedený v roku 1999. Od 802.11b sa odlišuje v mnohých technických parametroch a je s touto technológiou aj s jej nástupcami, teda variantmi g a n celkom nekompatibilný. (8)

Kým varianty b a g sa veľmi rýchlo šírili v Európe, štandard 802.11a si získal široké uplatnenie najmä v USA. Zásadný rozdiel je v použitom frekvenčnom pásme: 802.11a využíva pásmo 5 GHz, ktoré je tiež bezlicenčné, ale technické riešenie spoľahlivých prenosov je pri tejto frekvencii náročnejšie. Výhodou ovšem je, že toto pásmo je oproti pásmu 2,4 GHz relatívne „čisté“, je málo používané a preto takmer nezarušené. Maximálna teoretická komunikačná rýchlosť tohto štandardu je 54 Mbit/s. (8)

Základný protokol, na ktorom varianta a pracuje je zhodný so základným štandardom IEEE 802.11, ale používa OFDM moduláciu, pričom sa prenosové pásmo delí na 52 sub-kanálov. 4 sub-kanály sú „pilotné“ a 48 sub-kanálov je určených na prenos dát. (8)

Každý sub-kanál je modulovaný niektorou z dostupných modulačných techník nižšej úrovne a to BPSK, QPSK, 16-QAM alebo 64-QAM. Od použitej modulačnej techniky potom závisí prenosová rýchlosť, ktorá je odstupňovaná hodnotami 6, 9, 12, 18, 24, 36, 48 a 54 Mbit/s. Celková šírka prenosového pásma pre túto špecifikáciu je 20 MHz, delí sa do 12 neprekrývajúcich sa operačných kanálov. (8)

Skutočne využitých je 16,6 MHz (zvyšok je potrebný rezervovať ako „medzery“ medzi sub-kanálmi), na jeden sub-kanál potom pripadá 0,3125 MHz. Na prenos jedného symbolu sú potrebné 4 mikrosekundy, medzera medzi symbolmi je 0,8 mikrosekundy. (8)

2.3.4 IEEE 802.11n

V januári 2004 prichádza ďalší štandard 802.11n, ktorý môže teoreticky dosiahnuť prenosovú rýchlosť až 540 Mbit/s a v otvorenom priestore je možné sa pripojiť zo vzdialenosti približne 250 metrov, v uzavretom priestore je to necelých 100 metrov. (8)

Zvýšenie prenosovej rýchlosti je dosiahnuté technológiou multiple-input multiple-output (MIMO), ktorá na prenos dát využíva súčasne viacero prístupových bodov a viacero trás. Efektívnejšie využitie prenosového pásma je dosiahnuté novým kódovacím mechanizmom – tzv. like Alamouti coding. (8)

Štandardy 802.11b ani g neriešia problematiku prideľovania pásma podľa potrieb aplikácií ani nezaisťuje kvalitu služieb (QoS), čo je dôležité najmä pre multimediálne prenosy. Problematická je aj bezpečnosť komunikácie, pretože v prípade rádiových prenosov je mimoriadne jednoduché signál zachytiť a spracovať. Z týchto dôvodov sa IEEE zaoberá radom doplnkov k I EEE 802.11 (802.11d, e, f, h, i, j). (8)

Tabuľka 1. Prehľad štandardov IEEE 802.11 (Dostupné na (10))

Štandard	Pásmo [GHz]	Maximálna rýchlosť [Mbit/s]	Fyzická vrstva
IEEE 802.11 (pôvodný)	2,4	2	DSSS
IEEE 802.11a	5	54	OFDM
IEEE 802.11b	2,4	11	DSSS
IEEE 802.11g	2,4	54	OFDM
IEEE 802.11n	2,4 a 5	540	OFDM, MIMO

2.4 Doplnky štandardov 802.11

2.4.1 IEEE 802.11d

Obecné problémy medzinárodných použiteľností. (1)

2.4.2 IEEE 802.11e (Quality of Service)

QaS, ako je tento protokol známy odborníkom na riadenie sietí, udeľuje niektorým dátovým paketom prioritu pred inými paketmi. QaS sa považuje za kritický faktor pre vytvorenie takej robustnej normy 802.11, ktorá by bola vhodná pre hlasovú a dátovú komunikáciu, taktiež aj pre multimediálne aplikácie. (2)

2.4.3 IEEE 802.11h (Spectrum Manager 802.11a)

Na rozdiel od ethernetu nie sú bezdrôtové siete dobrými poslucháčmi. Zatiaľ čo zariadenia používajúce ethernet prevádzajú pozdržanie dátového prenosu, kým nezískajú istotu, že je médium voľné, 802.11 prevádza prenos ľubovoľne a nečaká na odozvu od stanice alebo prístupového bodu. Výsledkom je ak preťažená sieť, tak potenciálne rádiové rušenie. Pretože má tento problém vplyv na všetky normy 802.11, pracuje pracovná skupina H špecificky a doplnení 802.11a. (2)

2.4.4 IEEE 802.11f

IAPP (Inter-Access Point Protocol, roaming medzi AP). (1)

2.4.5 IEEE 802.11i (Enhanced Security)

Bezpečnostné protokoly (WEP, 802.11x, AES a ďalšie). (1)

2.5 Jednotlivé druhy prenosov na úrovni fyzickej vrstvy

2.5.1 FHSS

Fyzická vrstva, založená na FHSS, má k dispozícií 22 modelov (skokové sekvencie). Na tejto fyzickej vrstve je definovaných 79 kanálov v okolí frekvencie 2,4 GHz. Jeden kanál zaberá šírku pásma 1 MHz a preskakuje minimálne 2,5krát za sekundu, typicky 20krát. (14)

2.5.2 DSSS

Oba popisované systémy majú definovanú vlastnú inicializačnú sekvenciu bitov, aby prijímač bol schopný rozpoznať použitý modulačný formát a očakávanú dĺžku dátového reťazca. (1)

DSSS používa 11 kanálov o šírke 22MHz. Povolené pásmo na frekvencii 2,4 GHz má však šírku iba 83,5 MHz, takže takéto rozdelenie na kanály je možné len vďaka tomu, že stredné kmitočty jednotlivých kanálov sú od seba posunuté iba o 5 MHz. Tým pádom je získaných viac kanálov, avšak prekrývajúce sa kanály sa navzájom rušia. (1)

Hlavnou výhodou DSSS oproti FHSS je podpora vyšších rýchlostí. DSSS vysiela na jednom frekvenčnom kanáli, pričom dáta vysiela viackrát, tým je zaistená robustnosť prenosu dát a je znemožnené ľahké rušenie úzkopásmovým vysielačom. (1)

2.5.3 Infračervený prenos

Aj keď bol infračervený prenos (IR) štandardizovaný v protokole 802.11, nenašiel sa žiaden komerčne dostupný výrobok, ktorý by ho plne využíval. Jeho hlavnou nevýhodou bolo nemožnosť prechádzať stenami. Avšak bol veľmi odolný voči rádiovému rušeniu. V dobe, keď tento štandard vznikal, ale bolo možné sa domnievať, že IR prenos by mohol byť populárny množstvom prenosov dát. Hlavným dôvodom bol cenový rozdiel medzi infračervenými a rádiovými adaptérmi, výrobná cena infračervených adaptérov bola v tej dobe až päťnásobne nižšia. Výrobcovia však na trh prišli s veľkou výrobou a sortimentom rádiových adaptérov, čo znamenalo ich prudký pokles cien a rádiové adaptéry plne prevalcovali infračervené. (4)

2.6 Šírenie rádiového signálu

Pri šírení rádiového signálu vstupuje do hry značné množstvo faktorov, ktoré môžu šírenie signálu komplikovať. A WiFi siete nie sú výnimkou. Obecne platí pravidlo, že medzi WiFi anténami by mala byť priama viditeľnosť. Čo je často veľmi obťažné splniť. (4)

Rádiový signál sa musí vyrovnať s týmito základnými problémami:

- Rušenie inými systémami v rovnakom pásme;
- Priama viditeľnosť;
- Vplyvy počasia. (4)

2.6.1 Rušenie inými systémami v rovnakom pásme

Asi najdôležitejší vplyv na prenos rádiového signálu má rušenie inými zariadeniami v rovnakom frekvenčnom pásme. Kde predstavujú najväčšiu hrozbu systémy postavené na modulácii FHSS, napríklad technológie Breeze Net. Táto technológia vysiela krátke

signály do celého pásma ISM, čo vedie k charakteristickým niekoľkosekundovým výpadkom WiFi spojenia všade tam, kde na seba tieto technológie narazia. (4)

Ďalšie rušenie môžu predstavovať iné WiFi zariadenia. Kvôli šírke kanálu 22 MHz a odstupu medzi jednotlivými kanálmi poskytuje WiFi pásmo celkom iba tri oddelené fyzické kanály, a to kanály 1, 6 a 11. Keď sú zdroje rušenia vo väčšej vzdialenosti, nevadí, že sú aj na kanále, ktorý sa prekrýva s použitým kanálom, v niektorých prípadoch je ale vhodné kontaktovať prevádzkovateľa susedného WiFi zariadenia a dohodnúť sa s ním na „harmonizácií“ frekvenčného rozsahu tak, aby si navzájom čo najmenej prekážali. (4)

Rušenie z mikrovlnných rúr nie je veľký faktor pokiaľ signál neprechádza priamo rúrou. V súčasnosti sú rúry dobre odtienené, preto nepredstavujú takmer žiadne riziko. Horšie to môže byť so zariadeniami bluetooth a bezdrôtovými telefónmi. Bezdrôtové telefóny u nás frekvenciu 2,4 GHz nesmú používať. DECT (digitálny komunikačný štandard) sa pohybuje v pásme 1,9 GHz, ale dovozom z východu sa k nám mohli dostať aj zariadenia pracujúce v tomto pásme. Bluetooth sa u nás síce šíri celkom rýchlo, ale vďaka minimálnemu vysielaciemu výkonu od neho nehrozí mnoho rizík. (4)

2.6.2 Priama viditeľnosť

Priama viditeľnosť medzi WiFi anténami znamená, že je možné z miesta umiestnenia jednej antény vidieť okom na druhú anténa. Keď to nie je možné je pravdepodobné že nastanú problémy zo signálom. Rozdiely sú predovšetkým v tom, aký materiál a aká hrúbka materiálu stojí v ceste. Je nemožné, že zo vstavanou anténou prístupového bodu bude pokrytie veľkej budovy zo železobetónu, alebo pokryť suseda v panelovom dome kvalitné. O niečo lepšie je to s tehlovými stenami, v ktorých sa nenachádza oceľ ako v železobetóne či paneloch. Najlepšie sú v súčasnosti sadrokartónové steny, ale aj tie predstavujú určité percento rušenia. Tienenie stromov predstavuje tiež veľké percento rušenia čo sa často nedoceňuje a najmä keď sa meranie prevádza v lete, alebo v zime, keď na stromoch nie je lístie. (4)

2.6.3 Vplyv počasia

Počasie spôsobuje pri WiFi len mimoriadne malé výchylky, ale na dlhšie vzdialenosti je lepšie ho do kalkulácií zahrnúť. Pri prudkom daždi (cca 100 mm^3/hod) poklesne o 0,05 dB/km, pri bežnom daždi o 0,02 dB/km. U pásma 5,8 GHz je to o niečo horšie, 0,5 dB/km v prípade prietrže mračien až po 0,07 dB/km v prípade bežného dažďa. Nepríjemný problém nastane v prípade, že v ceste signálu stoja stromy, ktoré keď namoknú predstavujú pre signál veľkú prekážku. (4)

2.7 Topológie siete

WiFi siete používajú dve topológie teda usporiadanie a štruktúru danej siete. Základný súbor služieb (Basic Service Set) pre siete pozostávajúce zo zariadení, ktoré sú všetky vo vzájomnom dosahu alebo v dosahu jedného prístupového bodu (Acces Point). Siete s rozšíreným súborom služieb (Extended Service Set) umožňujú prekrývanie väčšieho počtu prístupových bodov, čo značne rozširuje rozsah jednej siete. ESS sa skladá z niekoľkých BSS. (2)

2.7.1 BBS

Existujú dva typy sietí BSS:

- Ad-hoc siete (tiež nazývame ako nezávislé siete alebo peer-to-peer siete);
- Infraštruktúrne siete. (2)

Ad-hoc sieť pozostáva z počítačov alebo iných WiFi zariadení, ktoré medzi sebou komunikujú priamo. Naproti tomu infraštruktúrna sieť sa skladá z prístupového bodu, ktorý riadi komunikáciu a zabezpečenie pre zariadenia, ktoré sú k nemu pridružené. Všetka komunikácia medzi zariadeniami na infraštrukturnej sieti vedie cez prístupový bod. Aj vtedy keď sú dva notebooky fyzicky veľmi blízko, bližšie, než je ich vzdialenosť od prístupového bodu danej siete, putujú signály od vysielajúceho

notebooku k prístupovému bodu a potom k prijímaciemu zariadeniu. WiFi zariadenia nemôžu byť súčasne v ad-hoc a infraštruktúrnej sieti. Ad-hoc siete sa hodia pre dočasné spojenie medzi počítačmi, alebo pre siete obsahujúce len pár bezdrôtových zariadení. (2)

Infraštruktúrne siete sa oproti tomu z dvoch dôvodov hodia lepšie pre trvalé bezdrôtové siete. (2)

Prvým dôvodom je, že prístupový bod uľahčuje pripojeným zariadeniam zdieľanie prístupu na internet. Počítače, ktoré sa chcú pripojiť do siete, sa musia autentizovať voči prístupovému bodu, inak nebudú mať prístup k ďalším zariadeniam na sieti. (2)

Druhým dôvodom je, že infraštruktúrna sieť BSS poskytuje väčší dosah než ad-hoc sieť,, alebo mobilné zariadenia nesmú byť vo vzájomnom dosahu. Namiesto toho každé zariadenie musí byť v dosahu prístupového bodu. To umožňuje, aby napríklad zariadenia, ktoré nie sú vo vzájomnom dosahu, si vymieňali zdieľané súbory, kým budú oba tieto zariadenia v dosahu prístupového bodu. (2)

2.7.2 EES

Je vytvorená v prvom rade pripojením každého prístupového bodu k chrbticovej sieti určitého druhu. Touto sieťou by mohla byť a obvykle aj je ethernetová sieť alebo nie aký druh siete s komunikačným médiom spojovej vrstvy (2.vrstva OSI modelu). Táto káblová sieť môže fungovať len pre zaistenie spojenia prístupových bodov alebo môže bezdrôtovému ESS poskytovať prístup na internet a služby lokálnej siete. (2)

Prostriedkom, ktorým prístupové body komunikujú medzi sebou, je distribučný systém (DS). Prístupové body pracujú v rámci ESS ako mosty medzi sieťami BSS, ktoré tvoria ESS, pričom umožňujú každej stanici na danej sieti komunikovať s akoukoľvek inou stanicou a ďalej umožňujú pohyb zariadení medzi segmentmi danej siete. To však bude fungovať iba vtedy, keď budú všetky prístupové body nakonfigurované ako členovia tej istej siete. Schopnosť prístupových bodov

komunikovať týmto spôsobom je stanovená v norme 802.11 a je označená ako DS. Všetky prístupové body dostávajú rovnaký názov siete a rovnaké nastavenie bezpečnostného prístupu, ale každý komunikuje na inom rádiovom kanále. Toto sa deje za účelom obmedzenia rušenia medzi prístupovými bodmi. Keď sa nie aké zariadenie dostane mimo dosah prístupového bodu, ku ktorému bolo pôvodne pridružené, prebehne automaticky jeho nové pridruženie k inému prístupovému bodu, pokiaľ je taký bod v dosahu a pokiaľ tento prístupový bod môže prijímať nové stanice. Z hľadiska návrhu siete je vhodné umiestniť prístupové body tak, aby sa ich oblasti pokrytia prekrývali, čím sa zabráni medzerám v prístupe pre pohybujúce sa stanice. (2)

2.8 Výhody bezdrôtových sietí

- WiFi siete na rozdiel od paketových rádiových systémov využívajú nelicencované rádiové pásmo;
- WiFi je bezdrôtová sieť, preto umožňuje vybudovať LAN sieť bez pomoci káblov, tým pádom je cenove menej náročná;
- Veľký sortiment produktov a kompatibilita medzi výrobcami;
- Veľká konkurencia medzi výrobcami znižuje ceny produktov;
- WiFi siete podporujú tzv. roaming, vďaka ktorému sa môže mobilná klientska stanica presunúť od jedného prístupového bodu k druhému bez straty spojenia súčasne s pohybom používateľa v budove alebo oblasti;
- Podpora rozličných stupňov kryptovania, vďaka čomu je komunikácia zabezpečená pred zachytením neželanou osobou.(8)

2.9 Nevýhody bezdrôtových sietí

- Použitie WiFi pásma 2,4 GHz vo väčšine krajín nevyžaduje licenciu za predpokladu, že zostáva pod limitom 100 mW a akceptuje rušenie z iných zdrojov vrátane rušenia, ktoré zapríčiní znefunkčnenie zariadení;
- Pásma a operačné obmedzenia nie sú na celom svete rovnaké. Dá sa povedať že každý väčší štát používa iné kanály;
- WiFi štandardy 802.11b a 802.11g používajú nelicencované pásmo 2,4 GHz, ktoré je preplnené inými zariadeniami, ako napríklad bluetooth, mikrovlnné rúry, bezdrôtové telefóny alebo zariadenia na bezdrôtový prenos video signálu. To môže spôsobiť zníženie výkonu, avšak mnohé adaptéry majú zabudované algoritmy odolné voči mikrovlnnému rušeniu;
- Vysoká potreba v porovnaní s niektorými inými štandardmi znižuje životnosť batérií a spôsobuje prehrievanie zariadení a k následnom poklesu životnosti;
- Na starších zariadeniach najpoužívanejší bezdrôtový kryptovací štandard Wired Equivalent Privacy (WEP) je prelomiteľný, aj keď je správne nakonfigurovaný, príčinou je generovanie slabého kľúča;
- Obmedzený dosah WiFi. Typický domáci WiFi smerovač používajúci 802.11b alebo 802.11g môže mať dosah cca 45 m v budove a 90 m mimo budovy;
- Prístupové body sa dajú využiť na ukradnutie osobných informácií vysielaných WiFi klientmi;
- Bezplatné prístupové body alebo nesprávne nakonfigurované prístupové body môže záškodník využiť na anonymný útok, ktorý sa nedá vystopovať;
- Oveľa menšia prenosová rýchlosť ako pri metalických alebo optických kábloch. (8)

2.10 Bezpečnosť bezdrôtových sietí

Bezdrôtová sieť má oproti káblovej sieti jednu výraznú nevýhodu pretože nie je možné zamedziť priestor, kde sa signál šíri teda je možné ho odpočúvať. Na odpočúvanie v káblovej sieti, je potreba sa fyzicky dostať ku jej káblom. K odpočúvaniu bezdrôtovej sieti sa stačí dostať do priestoru, kde sa tento signál dá zachytiť. (4)

Moderné prepínače na viac v káblových sieťach posielajú na jednotlivé počítače, tok dát určený len istým počítačom a tým sťažujú prienik do káblovej siete a jej odpočúvanie. V bezdrôtovej sieti je možné zachytiť tok dát všetkými bezdrôtovými zariadeniami. Pomocou programov ľahko dostupných z Internetu je možné z počítačov pripojených pomocou WiFi snifovať, zachytávať heslá a ďalšie dáta, pokiaľ nie sú šifrované. (4)

Môže sa zdať, že zabezpečenie WiFi siete nie je dôležité v prípade, že sa v nej nepracuje s citlivými dátami a že napríklad pre stavbu komunikačnej siete, v ktorej sa delí pripojenie na Internet medzi užívateľmi, nie je potreba sa zabezpečením zaťažovať. Nie je to ale pravda, pretože k zabezpečeniu siete patrí aj riadenie prístupu do nej, a aj to, aby pripojenie k Internetu mohli používať len ľudia, ktorým to umožňuje prevádzkovateľ siete, napríklad keď niekto platí za pripojenie. (4)

Bezpečnosť bezdrôtových sietí je možné rozdeliť do dvoch hlavných skupín:

- Šifrovanie, teda zabezpečenie prenášaných dát pred odpočúvaním;
- Autorizácia, teda riadenie prístupu oprávneným užívateľom. (4)

WiFi sieť už v svojom štandarde 802.11 obsahuje možnosť šifrovať dáta. Je to samozrejmý predpoklad k tomu, aby bolo WiFi dôveryhodné pre užívateľov. Sú tu ale isté dosť podstatné obmedzenia, dané predovšetkým historickým vývojom. (4)

2.10.1 Service Set Identifier

Je to jedinečný identifikátor každej bezdrôtovej WiFi počítačovej siete. Keď prístupový bod vysiela pravidelne každých niekoľko sekúnd svoj identifikátor v takzvanom rámci a klienti si tak môžu ľahko vybrať, ku ktorej bezdrôtovej sieti sa pripoja. (11)

Parameter SSID sa skladá z reťazca ASCII znakov dlhého maximálne 32 znakov. Tento parameter predstavuje, kľúč ktorým dochádza k spojeniu jednotlivých zariadení v rámci bezdrôtovej siete. Všetky bezdrôtové zariadenia pokúšajúce sa o vzájomnú komunikáciu medzi sebou musia posúvať ten istý SSID. Keby že sa kľúč klientskeho zariadenia nezhodoval s kľúčom prístupového bodu je prístup automaticky odmietnutý. (11)

SSID na bezdrôtových klientoch je nastavený automaticky, alebo manuálne vstupom do klientskeho módu nastavenia. Názov je obvykle nastavený k pomenovaniu sieťového operátora, ako napríklad názov spoločnosti. Hodnotou parametru SSID v sieti je treba považovať na prvú úroveň zabezpečenia. Pri kúpe nového zariadenia je SSID defaultne dané a je potrebné voči bezpečnosti si ho zmeniť. (11)

Tabuľka 2. Defaultné hodnoty SSID v bezdrôtových sieťach (Dostupné na (11))

Výrobca	**Základné hodnoty SSID**
3Com	101, comcomcom
Cisco	Tsunami, WaveLAN Network
Compaq	Compaq
Dlink	WLAN
Intel	101, 195, xlan , intel
Linksys	Linksys, wireless
NetGear	Wireless
SMC	WLAN
Symbol	101
Teletronics	any
Vigor	default
Zcomax	any
Zyxel	Wireless
Ostatné	Wireless

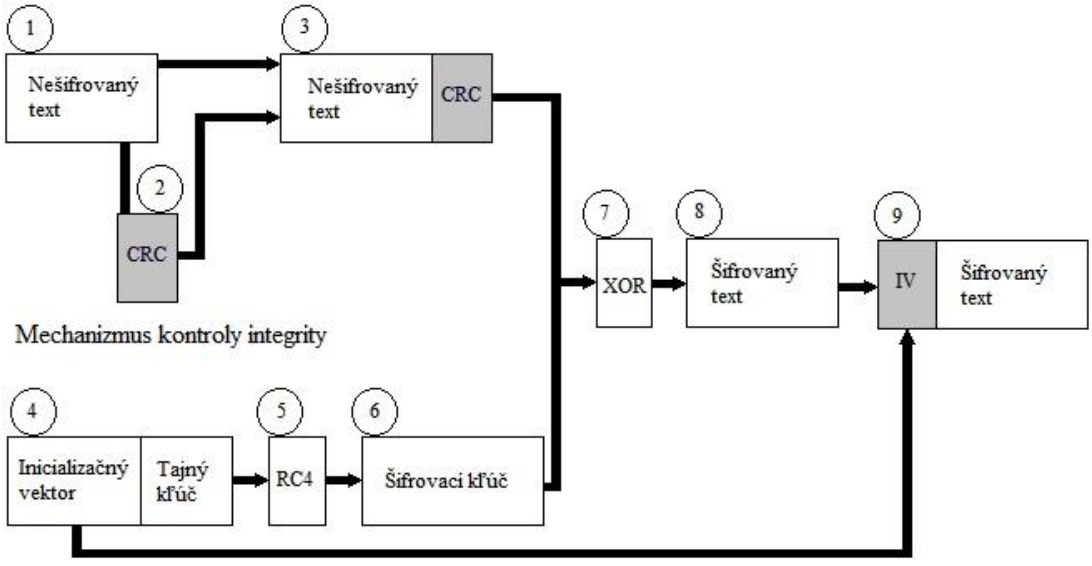
Veľmi výhodná vlastnosť niektorých prístupových bodov vyššej triedy je podpora „viac SSID“ teda mnohonásobnej SSID. Každé SSID je naviazané na samotnú bezdrôtovú sieť, takže je možné vytvárať veľmi rafinované bezpečnostné profily. Napríklad verejné SSID sa bude mapovať na bezdrôtovej sieti s nie akou sadou bezpečnostných pravidiel, privátne SSID sa bude mapovať s úplne inak nastavenou sadou pravidiel. (1)

Vďaka podpore viac SSID sa zároveň značne uľahčuje správa frekvenčného pásma. V minulosti platilo, že pokiaľ bolo potrebné prepojiť niekoľko bezdrôtových sietí k samotnej káblovej sieti, musela mať každá taká sieť vlastný prístupový bod. Tým sa však veľmi komplikuje správa pásma a zvyšujú sa náklady vďaka nutnosti inštalovať duplicitné zariadenie. Keď sa použije prístupový bod s podporou viac SSID, ktoré dosiahne potrebné usporiadanie s jedným prístupovým bodom a jedným kanálom. (1)

2.10.2 Šifrovanie dát algoritmom WEP

Šifrovanie pomocou algoritmu Wired Equivalent Privacy vzniklo z roku 1999. Prebieha spôsobom šifrovania rámcov. Jeho zámerom je zaistiť užívateľom do istej miery bezpečnosť, čo nie je príliš dôkladné . WEP nebol navrhnutý ako finálne bezpečnostné riešenie pre bezdrôtové siete. Obsahuje veľké množstvo nedostatkov, vďaka ktorým je náchylný na niekoľko typov útokov. (1)

Proces šifrovania vždy začína nešifrovaným textom, ktorý chceme chrániť. Najprv WEP z tohto textu vypočíta 32bitový cyklický redundantný súčet (CRC), teda kontrolný súčet pre overenie integrity dát. Tento kontrolný súčet sa následne pripojí za prenášanú správu. Ďalej vezme tajný kľúč a pripojí ho k inicializačnému vektoru (IV). Kombinácia IV a tajného kľúča posunie do generátora pseudonáhodných čísel RC4 (PRNG) a výstupom bude šifrovací kľúč. Šifrovací kľúč je sekvencia núl a jednotiek rovnako dlhá ako pôvodná správa plus kontrolný súčet. Následne medzi textom spojeným s kontrolným súčtom a šifrovaným kľúčom je prevedený logický výhradný súčet (XOR). Výsledkom je šifrovaný text, pred ktorý je ešte pripojená hodnota inicializačného vektora. (1)



Obrázok 1. Šifrovanie protokolom WEP (Dostupné na (1))

Dešifrovanie prebieha rovnako ako šifrovanie, ale samozrejme obrátene. Inicializačný vektor, ktorý je súčasťou prijatej správy, ku ktorému je pripojený tajný kľúč a výsledok je posunutý generátoru RC4, ktorý znovu vytvorí sekvenciu šifrovacieho kľúča. Medzi týmto kľúčom a zašifrovanou správou je ďalej prevádzaná operácia XOR, čím sa získava pôvodná hodnota. Znovu sa pre ňu vypočíta kontrolný súčet a porovná zo súčtom, ktorý sa priradil. Kebyže sa kontrolné súčty nezhodovali, predpokladá sa poškodenie správy a zahodí sa. (1)

WEP je náchylný na útoky typu replay, podvrhnutie/zmeny správy, ale najmä k odhaleniu kľúča obyčajným odposluchom a hrubou silou, pretože kľúč (u 24bitového IV dochádza skoro k opakovaniu) a šifra RC4 sú veľmi slabé. (3)

Bezpečnosť siete s WEP sa dá narušiť ľahko ak mechanicky (krádežou jedného z koncových zariadení s príslušnou WiFi kartou), tak aj odposluchom. Na základe odposluchu je možné kľúče ľahko zlomiť iba za pomoci notebooku, karty pre 802.11 a verejne dostupného softwaru (napr. AirSnort, WEPcrack). Ako náhle dôjde k narušeniu bezpečnosti, krádeži alebo odhaleniu kľúča, musí sa vykonať kompletná zmena kľúčov a všetkých zariadení v danej sieti zdieľaných rovnaký kľúč. (3)

WEPplus je vylepšenie pôvodného WEP zabezpečenia od Agere Systems, ktoré sa snaží odstrániť takzvané slabé inicializačné vektory. Sú to tie inicializačné vektory, pomocou ktorých môže útočník veľmi rýchlo spočítať použitý kľúč a tak sa môže do siete zabezpečenej pomocou WEP pripojiť. Pokiaľ nie je WEPplus na všetkých komunikujúcich stranách v bezdrôtovej sieti, nemá toto zabezpečenie oproti bežnému WEP žiadne výhody. (12)

WEP2 je vylepšenie pôvodného WEP, ktoré sa snaží odstrániť bezpečnostné diery. WEP2 rozšíril inicializačné vektory a zosilnil 128bitové šifrovanie. Bol typicky na zariadeniach, na ktorých nebolo možné prevádzkovať WPA alebo WPA2 zabezpečenie. Toto zabezpečenie má rovnaké bezpečnostné problémy ako WEP, len útočníkovi zaberie viac času pri infiltrácií. (12)

2.10.3 802.1x a EAP

Je to protokol umožňujúci autentizáciu na portoch, teda na fyzickej vrstve zariadení. Aj keď tento štandard nebol pôvodne určený pre bezdrôtové siete, je možné ho použiť k významnému zlepšeniu bezpečnosti v prostredí 802.11 a taktiež môže chrániť fyzické porty u káblovej sieti. Je to tak povediac blokátor portov, ktorý blokuje premávku až do doby, než sa klient autentizuje prostredníctvom údajov, ktoré sú uložené na back-end serveri, ktorým je typický RADIUS. (1)

RADIUS (Remote Authentication Dial-In User Service), ktorý zodpovedá za overovanie užívateľov pred prístupom do siete. Pracuje na princípe klient-server, kde klienti sú prístupové servery (NAS, Network Access Server). Transakcie medzi RADIUS serverom a klientmi sa autentizujú prostredníctvom zdieľaného hesla (secret), ktoré sa nikdy neprenáša v sieti. Hesla užívateľov sa posielajú medzi klientmi a serverom zašifrované. (3)

Komunikácia pri použití RADIUS prebieha nasledovne:

- Vzdialený užívateľ naviaže spojenie zo serverom NAS, ktorý od užívateľa požaduje meno a heslo;
- Na základe obdŕžania mena a hesla od užívateľa vyšle NAS serveru RADIUS žiadosť RADIUS ACCESS_REQUEST;
- Požiadavka sa vyšle na server RADIUS, pokiaľ daný server neodpovedá, môže sa využiť alternatívny RADIUS server;
- Server RADIUS overí požiadavku a správnosť užívateľského mena a hesla na základe výzvy a odpovie správou obsahujúcou povolenie/odmietnutie prístupu pre daného klienta do siete, RADIUS ACCESS_ACCEPT/DENY. (3)

Protokol 802.1x vychádza z protokolu PPP (Peer-to-Point Protocol). PPP sa pôvodne používal u vytáčacích pripojeniach a neskôr u niektorých DSL modemoch a káblových modemoch. Protokol PPP funguje skvele, je ale obmedzený tým, že umožňuje autentizáciu založenú iba na kombinácií užívateľského mena a hesla. (1)

802.1x je založený na protokole EAP, ktorý bol pôvodne vyvinutý PPP LCP (Point-to-Point Protocol Link Control Protocol). Jedná sa o mechanizmus prenosu EAP paketov prostredníctvom spojovej vrstvy LAN. Správy EAP sa zapuzdrujú do rámcov 802.1x. Preto sa 802.1x označuje ako EAPOL (Extensible Authentication Protocol over LANs). (4)

Autentizácia protokolu 802.1x začína odoslaním rámca EAP Start klientom. Tým sa autentizátor dozvie, že niekto takpovediac „klope na dvere“. Autentizátor odpovie rámcom EAP Request/Identity, v ktorom sa identifikuje. Autentizátor túto správu predá autentizačnému serveru. Autentizačný server pošle autentizátorovi rámec EAP-Request, ktorý obsahuje nie akú výzvu alebo požiadavku, napríklad zadanie hesla. Autentizátor tento rámec predá žiadateľovi, ktorý naňho príslušným spôsobom odpovie. Autentizátor odpoveď prevezme a predá ju autentizačnému serveru. (1)

Následne prevedie autentizačný server overenie a odpovie autentizátorovi rámcom EAP-Success alebo Failure. Pokiaľ autentizátor dostane rámec EAP-Success, prepne autentizátor riadený port z neautorizovaného stavu do autorizovaného stavu a povolí normálnu sieťovú komunikáciu. Žiadateľ a autentizačný server spolu nikdy nekomunikujú priamo. O všetku komunikáciu sa stará a sprostredkováva autentizátor. Klient môže v sieti komunikovať až vo chvíli, keď sa úspešne autentizuje. (1)

2.11 Metódy EAP

Protokol EAP podporuje desiatky metód autentizácie avšak zvolenú metódu EAP musia podporovať všetky tri komponenty systému, teda žiadateľa, autentizátora a autentizačný server.

2.11.1 MD5

Predstavuje najnižšiu možnú úroveň zabezpečenia a najľahšie sa implementuje. Táto metóda, v pôvodnom protokole PPP označovaná ako CHAP, ja napadnuteľné celou

radou útokov vrátane relatívne jednoduchého slovníkového útoku. Na viac musia byť hesla na strane servera uložené v čitateľnej podobe, čo je nebezpečný problém. (1)

2.11.2 LEAP

Poskytuje ako vzájomnú autentizáciu, tak aj dynamickú obnovu WEPových kľúčov. Tento protokol navrhla v roku 2000 spoločnosť Cisco ako dočasné riešenie pred schválením štandardu 802.1x. V tej dobe, pred uvedením WPA, to bolo práve Cisco, kto sa zaberal robustnými a škálovateľnými bezpečnostnými riešeniami nahradzujúcimi protokol WEP a jeho známe slabiny. (1)

2.11.3 TLS

Predstavuje z pohľadu bezpečnosti najsilnejšie riešenie, jeho nasadenie je ale zároveň naj obťažnejšie. TLS poskytuje vzájomnú autentizáciu a dynamickú obnovu WEPových kľúčov. Protokol prostredníctvom infraštruktúry verejného kľúča (PKI) vytvára šifrovaný tunel, ktorým prebieha výmena autentizačných údajov. Respektíve, musia byť na strane servera aj na strane klientov nainštalované digitálne certifikáty. Dobré je to, že ide o riešenie poskytujúce naj vyššiu možnú mieru bezpečnosti a zlé je to, pretože vybudovať úplnú infraštruktúru podporujúcu PKI je veľmi komplikované. (1)

2.11.4 TTLS

Podporuje vzájomnú autentizáciu a dynamickú obnovu WEPových. Na rozdiel od TLS však TTLS vyžaduje certifikát len na strane servera, u klienta nie je potrebný. Klienti sa autentizujú prostredníctvom hesiel. TTLS je takmer rovnako bezpečný ako TLS, jeho nasadenie je ale omnoho jednoduchšie. (1)

2.11.5 PEAP

Tento protokol je veľmi podobný protokolu TTLS. Podporuje vzájomnú autentizáciu a dynamickú obnovu WEPových kľúčov a vyžaduje certifikát len na strane servera. Autentizácia klienta prebieha zabezpečeným kanálom. Prostredníctvom certifikátu dôjde k autentizácii servera a následne je možné použiť inú metódu protokolu EAP k autentizácii klienta. Je možné použiť PEAP a MS-CHAP verzie 2 a celý postup bude bezpečný, pretože komunikácia protokolom MS-CHAP prebieha v zabezpečenom tuneli. (1)

Tabuľka 3. Bežné metódy protokolu EAP (Dostupné na (1))

Metóda	Typická implementácia	Smer autentizácie	Generovanie WEPového kľúča	Obtiažnosť nasadenia	Miera bezpečnosti
MD5	heslo založené na výzve	jednosmerná	nie	nízka	slabá
TLS	certifikovaná obojsmerná autentizácia	vzájomná	áno	vysoká	najlepšia
TTLS/PEAP	certifikovaná autentizácia servera, iná autentizačná metóda pre klientov	vzájomná	áno	stredná	dobrá

2.12 Šifrovanie dát algoritmom WPA

Algoritmus WPA (WiFi Protected Access) bol prijatý koncom roku 2002 združením výrobcov WiFi Alliance. WPA bol prijatý ako dočasné riešenie do tej doby, kým bude schválený bezpečnostný doplnok normy IEEE 802.11i. (3)

WPA používa rovnaký šifrovací mechanizmus RC ako WEP. Napokon protokol použitý vo WPA (TKIP) má kôli svojej vyššej zložitosti určitý vplyv na výkonnosť zariadení, v porovnaní s WEP dosť zníži výkonnosť o 5-15%. (3)

Dá sa plne zlúčiť s 802.11i, ale ešte nezahrňuje také prvky normy ako bezpečné, rýchle predávanie stanice medzi prístupovými bodmi (secure fast handoff) na základe predbežnej autentizácie (pre-authentication), bezpečná deautentizácia a odpojenie alebo rozšírený protokol pre šifrovanie na bázi AES. Tie totiž už vyžadujú hardwarové zmeny v bezdrôtových produktoch. Výhodou sú dynamické kľúče, ale necháva sa tiež priestor pre statické zdieľané kľúče pre jednoduchšiu implementáciu napríklad v domácom prostredí. (3)

Tri zložky WPA:

- Temporal Key Integrity Protocol (TKIP): používa 40bitový kľúč ako WEP (s RC4), ale mení ho pre každý paket a bráni sa tak proti útoku hrubou silou, na viac sa zdvojnásobila dĺžka IV na 48 bitov;
- Message Integrity Check (MIC): prenos je chránený proti narušeniu, integrita dát je zaistená (ochrana proti falošným prístupovým bodom);
- Extensible Authentication Protocol (EAP): vzájomná autentizácia užívateľa a siete (ochrana proti falošným prístupovým bodom) a distribúcie kľúčov. (3)

Nové bezpečnostné mechanizmy v rámci WPA museli odstrániť zásadné nedostatky protokolu WEP, teda prakticky nulovú autentizáciu, a veľmi slabé šifrovanie statickým kľúčom. Autentizácia užívateľa na druhej vrstve je pre správcu siete veľmi dôležitá, pretože umožňuje presne špecifikovať užívateľov, ktorý môžu mať do siete prístup. Okrem jednosmernej autentizácie užívateľa voči sieti je potreba tiež užívateľom dať istotu, že sa pripojujú k autorizovanej sieti. Preto sa konečne prešlo na vzájomnú autentizáciu. (3)

WPA ponúka režimy autentizácie pre rôzne prostredia: v podnikovom prostredí predpokladá využitie centralizovaného autentizačného servera zodpovedajúceho za distribúciu kľúčov, zatiaľ čo v prostredí domácich sietí sa používa jednoduchší režim prednastaveného kľúča, kedy stanica tento kľúč zdieľa s prístupovým bodom a žiadne overovanie identity sa ďalej neprevádza. (3)

WPA plusy a mínusy

+ Rieši väčšinu známych slabín WEP;
+ Vhodné pre prostredie domácich sietí;
+ Implementácia.

– Staršie produkty nemusí byť možné vybaviť WPA;
– 802.1x potrebuje nákladnejšiu infraštruktúru;
– Súčasné aj nové typy EAP sa stále vyvíjajú. (3)

2.13 IEEE 802.11i (WPA2)

Tento štandard vylepšuje autentifikačný a šifrovací algoritmus bezdrôtových sietí WiFi. Bol schválený 24. júna 2004 a vyraďuje tak pôvodné zabezpečenie WEP, ktoré má mnoho bezpečnostných slabín. WPA je predchodcom WPA2, ale namiesto implementácie plného IEEE 802.11i implementuje iba 3. návrh tohto štandardu, teda iba podmnožinu 802.11i. Používa blokovú šifru AES (Advanced Encryption Standard), zatiaľ čo predchádzajúce WEP a WPA používajú prúdovú šifru RC4. (13)

Táto architektúra obsahuje komponenty: IEEE 802.1X pre autentizáciu (používa teda Extensible Authentication Protocol a autentizačný server), Robust Security Network (RSN) pre udržiavanie záznamu asociácií na AES založený na CCMP, ktorý poskytuje utajenie, integritu a autentizáciu. (13)

Tabuľka 4. Porovnanie vlastností WEP,WPA,WPA2 z hľadiska autentizácie a šifrovania (Dostupné na (3))

	WEP	WPA	WPA2
Autentizácia	otvorená	EAP-TLS alebo PEAP	EAP-TLS alebo PEAP
Šifrovanie	Statický WEP	TKIP/CKIP	AES

Tabuľka 5. Tab. Porovnanie vlastností WEP,WPA,WPA2 z hľadiska odolnosti útoku (Dostupné na (3))

	WEP	WPA	WPA2
Útok:	Odolnosť:		
Na integritu, dôverihodnosť dáť, man in the middle	dobrá	lepšia	najlepšia
Falošná autentizácia	nič moc	najlepšia	najlepšia
Na slabý kľúč	nič moc	najlepšia	najlepšia
Falošné pakety	minimálna	najlepšia	najlepšia
Falošný prístupový bod	minimálna	lepšia	lepšia
Úroveň šifrovania	pre domácu sieť (40 alebo 104bitový kľúč; 24bitový vektor IV)	pre podnikovú sieť (128bitový kľúč; 48bitový vektor IV)	Pre podniky a vládu (128+bitový kľúč; 48bitový vektor IV)

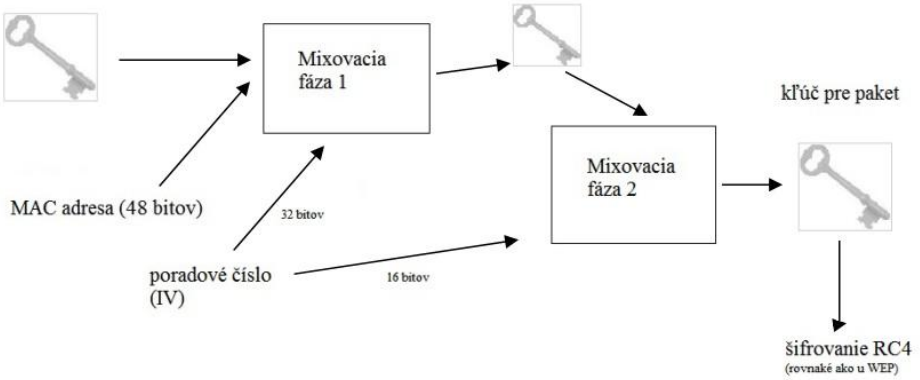
Tabuľka 6. Odporučenie pre nasadenie bezpečnostného riešenia v sieťach (Dostupné na (3))

	Autentizácia	Šifrovanie	Použiteľnosť pre podnik	Použiteľnosť pre domácnosť
WEP	nulová	WEP	nič moc	dobrá
WPA (PSK)	PSK	TKIP	nič moc	najlepšia
WPA2 (PSK)	PSK	AES-CCMP	nič moc	najlepšia
WPA (plná)	802.1x	TKIP	lepšia	dobrá
WPA2 (plná)	802.1x	AES-CCMP	najlepšia	dobrá

2.14 TKIP

Protokol TKIP (Temporal Key Integrity Protocol) je určený k riešeniu hlavných nedostatkov WEP. Obsahuje funkcie pre dynamické regenerovanie kľúčov, kontroly integrity správ a číslovania paketov na ochranu proti útokom typu replay. Tento protokol predlžuje dĺžku správy zašifrovanej pomocou WPA o 12 bajtov: 4 bajty pre rozšírenú informáciu IV a 8 bajtov pre kód integrity správy (MIC). (3)

TKIP vďaka 48 bitovému vektoru IV predĺženému oproti WEP zamedzuje možnému zneužitiu IV (útok FMS, kde ku kolízii IV muselo nutne dôjsť najneskôr po 4 miliónoch rámcov). IV má ovšem v tomto prípade dve úlohy, preto sa hodnota IV v skutočnosti delí na dve časti: 16bitová hodnota sa doplní do 24 bitov pre tradičnú IV a 32bitová časť slúži ako poradové číslo paketu a používa sa pre mixovanie kľúčov pre jednotlivé pakety. V prvej fáze sa zmieša dočasný kľúč relácie, 32 bitov IV a adresa MAC. V druhej fáze sa zmieša výstup prvej fázy s dočasným kľúčom relácie a 16bitovou časťou IV. Použije sa teda jednocestná funkcia hash, ktorá vedie vždy k jedinečnému kľúču. Dočasný kľúč relácie a MIC kľúč sa odvodzujú z kľúča PMK, ktorý sa dojednal v rámci 802.1x. (3)



Obrázok 2. Generovanie kľúča TKIP (Dostupné na (3))

2.15 AES-CCMP

AES je šifra podobajúca sa americkému federálnemu štandardu FIPS (Federal Information Processing Standards), ktorá bola navrhnutá ako náhrada RC4. Samotnému prijatiu šifry AES americkou vládou, predchádzal rozsiahly prieskum a revízie šifry. AES ponúka rôzne režimy činnosti, v špecifikácií 802.11 sa používa čítačový režim s protokolom CBC-MAC (CCM), obvykle označovaným ako AES-CCMP. Čítačový režim zaisťuje šifrovanie, CBC-MAC potom zaisťuje autentizáciu a integritu dát. (1)

Rovnako ako RC4 je aj AES šifra s rovnakým kľúčom, čo znamená, že sa text šifruje aj dešifruje rovnakým zdieľaným tajným kľúčom. Na rozdiel od šifry RC4, ktorá šifruje lineárne každý bajt XORovaním s náhodnou sekvenciou, AES pracuje s blokmi, ktoré majú veľkosť 128 bitov a preto sa označuje ako bloková šifra. (1)

CCMP aj TKIP majú kopu spoločných vlastností. Oba používajú 128bitový dočasný kľúč, odvodený od „master“ kľúča, ktorý sa získava v priebehu negociácie protokolom 802.1x. V terminológii CCMP sa 48bitová hodnota IV označuje ako „číslo paketu“ (PN). (1)

2.16 Kontrola prístupu pomocou filtrovania MAC adries

MAC (Media Access) adresa je identifikačné číslo sieťového adaptéra slúžiace na jednoznačnú identifikáciu sieťového rozhrania v lokálnych počítačových sieťach typu WiFi, Ethernet, Token Ring a mnohých ďalších. (5)

Je to spravidla 48-bitové číslo, ktoré sa pre prehľadnosť uvádza ako 12-miestne hexadecimálne číslo (napríklad. 08:00:69:02:01:FC, ako oddeľovače dvojíc sa používajú dvojbodky alebo pomlčky, prípadne sa číslo píše bez oddeľovania dvojíc, číslic). Každý sieťový adaptér (sieťová karta) má zaručenú jedinečnú MAC adresu. Jedinečnosť prvých troch bajtov (ID výrobcu) zaručuje IEEE, jedinečnosť posledných troch zabezpečujú jednotliví výrobcovia. (5)

Základná myšlienka filtrácie MAC adries je založená na tom, že sa v prístupovom bode udržuje zoznam autorizovaných MAC adries a povoľuje sa prístup iba tým zariadeniam ktoré sa nachádzajú v tomto zozname. (1)

Problém je však v tom, že kopa bezdrôtových kariet má k dispozícii ovládač, ktorý umožňuje užívateľovi MAC adresu zmeniť. Existujú aj iné nástroje, ktoré umožňujú meniť MAC adresu, napríklad SpoofMAC. Pretože sa zdrojová a cieľová MAC adresa posiela nešifrovane a to aj v prípade použitia WEP, môže útočník jednoducho odpočuť hodnoty povolených MAC adries a potom svoju bezdrôtovú kartu nastaviť tak, aby používala takúto platnú adresu. Keď sa karta tvári ako karta s povolenou MAC adresou, bude prístupový bod presvedčený o tom že ide o legitímne pripojenie. (1)

Okrem rizika falšovania MAC adries sa vo väčších sieťach stáva neudržateľná administrácia zoznamu autorizovaných adries. V malej kancelárii alebo v domácom prostredí sa filtrácia MAC adries implementuje ľahko, pretože sa jedná o nízky a viac menej konštantný počet klientov. Zmyslom tejto ochrany je predovšetkým to, že útočníkovi pravdepodobne nebude stáť za to sa trápiť s falšovaním MAC adresy, a že sa račej zameria na iný, menej chránený cieľ. (1)

2.17 Možné útoky na bezdrôtovú sieť

Väčšina metód sa odvíja od faktu, že oblasť pokrytia bezdrôtovou sieťou nie je možné fyzicky kontrolovať a zamedziť tak pohybu nežiaducim osobám. Najčastejšie používané metódy potenciálnymi útočníkmi z vonku, napríklad z ulice kde je možné signál zachytiť:

2.17.1 Rozlúštenie kľúča WEP

Lúštenie kľúča WEP je obľúbenou metódou útočníkov. K rozlúšteniu kľúča je potreba medzi 5 až 10 miliónov paketov a útočník spolieha na to, že celú dobu, keď ich bude zachytávať, WEP kľúč sa nezmení. Útočníci majú k dispozícii open source programy ako AirSnort alebo WEPCrack a stačí im zachytávať komunikáciu medzi prístupovým bodom a klientom. (4)

Obrana: Použiť šifrovanie a autentizačné mechanizmy pomocou VPN a 802.X. (4)

2.17.2 Zistenie MAC adresy

Adresa MAC pre pripojenie na prístupový bod sa zisťuje rovnako, ako sa dekóduje WEP kľúč. Pokiaľ nie je v sieti WEP aktivované, stačí útočníkovi zachytávať komunikáciu medzi prístupovým bodom a klientom a vyhľadať si hlavičku MAC adresy a tu si potom prečítať. Pokiaľ je WEP používaný, musí útočník najskôr dekódovať WEP, v tomto prípade mu ale postačuje aj offline analýza zachytených dátových rámcov. V okamihu, keď útočník získa MAC adresu, môže ju k svojej klientskej karte a vystupovať ako oprávnený užívateľ. (4)

Obrana: MAC útokom sa dá predchádzať použitím autentizačných mechanizmov ako 802.x a zabezpečenie na báze VPN. (4)

2.17.3 Útoky typu Muž u prostred

Tento útok je charakteristický tým, že hacker vstúpi medzi prístupoví bod a klienta a preruší pripojenie medzi nimi. Hacker zachytáva a dekóduje dáta prenášané medzi príslušným bodom a klientom behom asociačného prenosu. Takto získa základné informácie o klientovi aj o prístupovom bode, ako napríklad IP adresy oboch zariadení, asociačné ID klienta a SSID prístupového bodu. S týmito informáciami môže byť hacker schopný vytvoriť falošný prístupový bod bližšie k užívateľovi a zmeniť

pripojenie užívateľa na tento falošný prístupový bod. Dáta, ktoré na tento prístupový bod prijal, zaznamenáva a preposiela na skutočný prístupový bod, takže klient aj skutočný prístupový bod sa domnievajú, že spolu priamo komunikujú, zatiaľ čo v skutočnosti ich komunikáciu sprostredkováva a predovšetkým zachytáva „Muž u prostred“. Hacker sa takto dostáva ku všetkým dátam vrátane hesiel. (4)

Obrana: Použitie VPN a autentizačných mechanizmov 802.1x. Taktiež sa vyplatí mať podrobnú rádiovú mapu siete a občas prejsť, či niekde nevysiela nie aký prístupový bod, ktorý nie je v pláne a ktorý by mohol byť falošným prístupovým bodom. (4)

2.17.4 Slovníkový útok

Tento útok je založený na využití slovníku pre útok na užívateľské mená a hesla. Útočník sa snaží za pomoci databázy bežne používaných prihlasovacích mien a hesiel prelomiť šifru. Ako náhle sa mu podarí odhaliť správnu kombináciu, získava plný prístup do bezdrôtovej siete. Hackeri majú rôzne výhody v tom že existujú open source programy a databázy hesiel a prihlasovacích mien, ktoré je ľahké získať z internetu. Veľkou výhodou je, že sú anglofónne zamerané. (4)

Obrana: Hlavnou obranou je vhodne zvolené heslo, ktoré by malo pozostávať minimálne z 8 znakov a obsahovať aj čísla. Taktiež mechanizmus 802.1x. (4)

2.17.5 Denial Of Service

Tieto útoky nepatria medzi prieniky do siete, ide vlastne len o vyradenie funkčnosti siete. Útočník zahltí prístupový bod nezmyselnými dátami vo veľkom množstve. Prístupový bod sa snaží tieto dáta vyhodnotiť a dôjde k jeho zahlteniu prenosového pásma. To spomalí alebo úplne znemožní pripojenie ostatných užívateľov. (4)

Obrana: Filtrovanie MAC adries môže veľmi účinne brániť útokom DoS, pokiaľ sú tieto útoky vedené z Internetu, pomôže firewall s dobrou analýzou paketov. (4)

3 Analýza problému a súčasnej situácie

Bezdrôtové siete zažívajú po celom svete ohromný rast. Počet predaných jednotiek rapídne stúpa každým rokom a ich cena stále klesá. „WLAN“ ako je tento segment na trhu súhrnne označovaný, má podľa analytikov jeden z najvýraznejších stúpaní na IT trhu. Podľa dostupných údajov by mal tento trend aj v budúcom roku naďalej pokračovať. Podľa analytikov je tento rast podporený predovšetkým požiadavkami firemných užívateľov prenosových zariadení, teda notebookov, PDA a ďalších zariadení schopných komunikácie s okolitými zariadeniami, ako sú tlačiarne, a podobne. (9)

Od roku 2003 keď sa nasýtenie trhu pohybovalo okolo 9% do roku 2007 vystúpilo na neuveriteľných 90% a až do dnešku stále stúpa vplyvom nových a lacnejších zariadení, ktoré túto technológiu podporujú stále viac a viac. Podľa údajov došlo k najmasovejšiemu rastu hlavne v miestach s najväčším počtom prístupových buniek, tzv. Hotspotov, a lacnou konektivitou teda cenou za prípojku, predovšetkým v USA, Japonsku a celých ázisko-pacifických oblastiach. V Európe vďaka vyšším cenám za konektivitu to tempo bolo pomalšie. (9)

V Českej republike sa rast vyvíjal aj vďaka tomu že veľké spoločnosti ako O2 výrazne zlacňovali produkty umocňované masívnou kampaňou. Ale dnes má veľký počet sietí najmä vo väčších mestách problém udržať krok s konkurenciou a zažína stagnovať. Dôvodom nie je len vysoká konkurencia, ale hlavne vysoké zarušenie nelicencovaného pásma a najmä menšie siete, ktoré nedosiahnu na kvalitnejšie licencované technológie, čakajú v budúcnosti veľké problémy. To je tiež dôvod, prečo silné spoločnosti na trhu odkupujú slabšie stagnujúce spoločnosti. Otázkou ostáva koľko menších spoločností dokáže včas rozpoznať, že nastal ten správny čas kývnuť na predaj silnejšej spoločnosti, kým cena nie je príliš nízka a nehrozí bankrot. (7)

Avšak väčšina menších spoločností často krát ani nepozná svoju cenu a buď sa značne podhodnotí alebo naopak očakáva omnoho vyššiu ponuku, než je ktorýkoľvek väčší konkurent v blízkom okolí schopný ponúknuť. (7)

3.1 Analýza bezpečnosti

Káblové aj bezdrôtové LAN siete v súčasnosti čelia rôznym typom ohrozenia a majú rozdielne slabé stránky, iba 47% spoločností používa na svojich bezdrôtových sieťach kódovanie WEP alebo WPA, a menej než tretina teda 30% nepoužíva žiadny spôsob na ochranu svojej bezdrôtovej siete. (6)

V súčasnosti pri správe takýchto sietí sa čelí mnohým rozdielnym problémom. Napríklad 79% organizácií sa snaží podporovať vhodné bezpečnostné metódy tým, že používajú rovnaké IT postupy v rámci celej organizácie. Výskumom sa zistilo že 51% spoločností nemá žiadny spôsob, ako vo svojej sieti tieto postupy presadzovať. A na viac vzhľadom k tomu, že zamestnanci sú stále mobilnejší, môže sa stať, že vonkajšie siete a bezdrôtové hotspoty v kaviarňach budú predstavovať takzvané „zadné dvierka“ do bezpečného systému siete. 56% spoločností sa skutočne domnieva, že mnoho zamestnancov porušuje bezpečnostné opatrenia tým, že zasiela firemné dáta cez celkom nezabezpečené bezdrôtové siete, ako sú bezdrôtové hotspoty v kaviarňach namiesto toho, aby používali formu VPN. (6)

Pevná bezdrôtová bezpečnosť zahrňuje nielen prevenciu neautorizovaného prístupu k senzitívnym informáciám, ale tiež neustálou správou celého prostredia, ktoré identifikuje, izoluje a predchádza vzniku slabých bodov a možnému prieniku do siete, ktoré vyžaduje neustály monitoring a celkový dohľad nad sieťou. (6)

4 Vlastné návrhy riešenia, prínos návrhov riešenia

Doba, kedy sa bezdrôtový prenos informácií pre bežných užívateľov obmedzoval len na rozhlas, je už dávno minulosťou. Samozrejmý prechod na bezdrôtové technológie ako mobilné telefóny, televízia na diaľkové ovládanie sa nedal zastaviť. Podobne je tomu aj dnes, WiFi preniká do všetkých kútov spoločnosti, od podnikových riešení, cez domácich používateľov, školy a pracovísk. Je to prirodzený technický vývoj, kde vyhráva užívateľský komfort, mobilita a sloboda. Rapídny nárast produktov s technológiou WiFi v mobilných telefónoch priniesol veľké výhody pri pripojení sa do bezdrôtovej sieti.

Začiatkom celého projektu bol plán na vybudovanie bezdrôtovej sieti v centre pre deti, ktorý bol len otázkou času. Pretože takáto sieť uľahčí či už pripojenie zamestnancov a hlavne detí, ktoré navštevujú toto centrum.

4.1 Cieľ návrhu

- Zostrojiť stabilnú bezdrôtovú sieť;
- Pokrytie prvého poschodia signálom;
- Dostatočne zabezpečiť bezdrôtovú sieť pred možnými útokmi;
- Nákup kvalitných zariadení;
- Zaistenie kompatibility medzi produktmi.

4.2 Hardware a Software v centre

Centrum je vybavené priemernými stolnými počítačmi v kanceláriách zamestnancov. Počítače obsahujú operačný systém Windows XP. Tieto počítače sú v sieti LAN, ktorá tam funguje pár rokov. Preto nie je potreba vybavovať tieto počítače bezdrôtovým zariadením.

Riaditeľ centra vlastní súkromný notebook s WiFi technológiou, ktorý bol doposiaľ pripojený do LAN. Ale kôli flexibilite a mobilite sa rozhodlo že sa tento notebook môže pripojiť na WLAN.

LAN sieť tvorí switch, ktorý je pripojený na centrálny router od poskytovateľa prípojky internetu.

4.3 Použité zariadenia

Modelový „kit“ sa skladal z nasledovných zariadení:

- 1x Cisco Wireless LAN Controller 2106
- 2x Cisco 1000 Series AP (AIR-AP1010-E-K9)

4.4 Realizácia

Hlavný objekt je priestranná 2-poschodová budova. Celá architektúra sa nachádza na 1-poschodí, na ktorom sa vybudovala bezdrôtová sieť pomocou dvoch prístupových bodov. Dôvodom dvoch prístupových bodov bol fakt že budova je staršia a má hrubé steny.

Jeden sa nachádza v rohu spoločenskej miestnosti. Je to veľká priestranná miestnosť bez stien. Tento prístupový bod bol umiestnený kôli čo najlepšiemu bezdrôtovému signálu v ľavom hornom rohu a tak pokrýva polovicu budovy perfektným bezdrôtovým signálom.

Druhý prístupový bod sa nachádza v kancelárií riaditeľa. Tento prístupový bod pokrýva signálom druhú polovicu budovy teda aj kanceláriu zamestnancov. Tým pádom sieť LAN začína byť nepotrebná ale v budúcnosti sa rušiť nebude a počítače ostávajú do nej pripojené. Bezdrôtová sieť v týchto kanceláriách môže slúžiť pre osobné zariadenia zamestnancov a detí v budove.

Prístupové body Cisco AIR-AP1010-E-K9 ponúkajú funkcie:

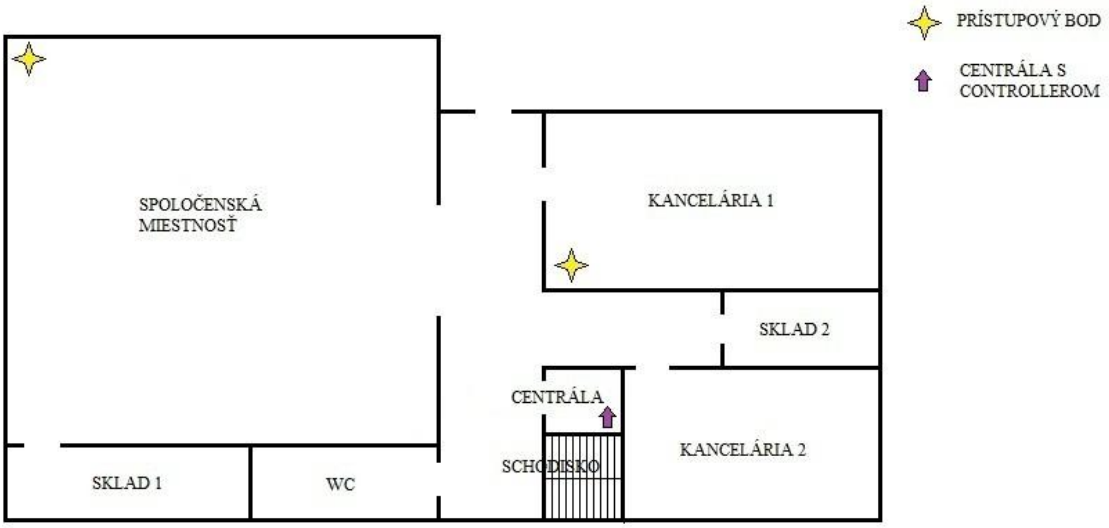
- Duálnych vysielačov, poskytujúcich podporu viacerých variantov bezdrôtových sietí vysielajúcich v pásmach 2,4 a 5 GHz pre najlepšiu flexibilitu, pokrytie a podporu klientskych zariadení;
- Schopnosti zabezpečiť pokrytie aj v prípade prekážok alebo rušenia;
- Ľahkej inštalácie na zavesený strop;
- Integrácie so softvérom na správu a monitorovanie bezdrôtových sietí spoločnosti Cisco.

Tieto prístupové body sú pripojené na takzvaný Controller, ktorý umožní centralizovanú správu a riadenie bezdrôtovej siete. Controller ponúka škálu týchto funkcií:

- Podpora viacerých kombinácií prístupových bodov a redundantných prepojení;
- Štandardných protokolov zabezpečenia, overenia identity a šifrovania na dosiahnutie najvyššej úrovne ochrany;
- Zabezpečeného prístupu s oprávneniami hosťa;
- Hlasových služieb prostredníctvom siete WLAN;
- Integrácie s ovládacím systémom Cisco Wireless Control System na úplnú konfiguráciu a sledovanie bezdrôtovej siete;
- Pohodlnej montáže do počítača alebo stojana skrine s routerom vďaka malým rozmerom radiča.

Jedná sa o centralizované riešenie, t.j. všetky prístupové body (AP) musia mať prístup ku controlleru, ktorý im poskytne konfiguráciu. Z uvedeného je jasné, že stredom topológie musí byť switch a k nemu pripojený controller. Model switchu, ktorý centrum vlastní podporuje Power-over-Ethernet, stačí od neho už len natiahnuť káble k vybraným polohám prístupových bodov. Konečné rozhodnutie o uložení „centrálu“ bolo do miestnosti pre upratovačky na 1 poschodí vedľa schodiska. Tým pádom sa zmenila funkčnosť tejto miestnosti na miestnosť s centrálou. Dá sa povedať že miestnosť sa nachádza takmer v pomyselnom strede budovy, čím sa dosiahlo, že najdlhší káblový prepoj má menej ako 50 metrov. Centrála sa zapája na uplink teda

prípojku od poskytovateľa Internetu ktorý zabezpečuje Cisco series 800 router (ten nieje súčastou projektu).



Obrázok 3. Plán poschodia (Zdroj vlastný)

Tabuľka 7. Základné parametre Cisco AIR-AP1010-E-K9

Porty	10/100 Mbps Ethernet
Technológie	QoS, Lightweight Access Point Protocol (LWAPP), auto MDI/MDIX
Modulácie	DSSS, OFDM
Max. rýchlosť	802.11a 54 Mbps, 802.11b 11 Mbps, 802.11g 54 Mbps
Bezpečnosť	WPA, 802.11i/WPA2
Napájanie	48 VDC, Power over Ethernet (IEEE 802.3af)

Obrázok 4. Cisco AIR-AP1010-E-K9 (Zdroj vlastný)

Tabuľka 8. Základné parametre Cisco Wireless LAN Controller 2106

Prenos dát	
Maximálna prenosová rýchlosť	0.1 Gbit/s
Rýchlosť prenosu dát	10/100 Mbit/s
Pripojenie do siete	
Vlastnosti siete	Ethernet/Fast Ethernet
Sieťový štandard	IEEE 802.3, IEEE 802.3u, IEEE 802.1Q, IEEE 802.3af, IEEE 802.1x, X.509
Management vlastnosti	
Typ prepínača	Managed
Quality of Service (QoS) support	Áno
Protokol	
Protokol dátového spoja	Ethernet, Fast Ethernet
Podporované sieťové protokoly	TCP/IP, UDP/IP, ICMP/IP
Možnosti prepojenia	
Počet portov	8
Bezpečnosť	
Podpora bezpečnostných algoritmov	RSA, RC4, MD5, AES, 128-bit WEP, SSL, TLS 1.0, 104-bit WEP, TKIP, WPA, WPA2, PKI, AES-CCMP

Obrázok 5. Cisco Wireless LAN Controller 2106 (Zdroj vlastný)

4.5 Konfigurácia zariadení

Výhoda centralizovaného riešenia je v zjednodušení a urýchlení konfigurácie. V našom prípade stačilo nastaviť SSID, metódu autentizácie a enkrypcie. Vzhľadom na to, že všetky prístupové body sú vo vnútri budovy a neboli použité žiadne externé antény, pokrytie signálom mimo budovy bolo minimálne. Zároveň je predpoklad, že v tomto centre pre deti sa budú nachádzať iba osoby, ktoré majú povolený prístup k bezdrôtovej sieti.

Ako sa už neraz potvrdilo, najlepšou metódou informatizácie spoločnosti je umožniť ľudom prístup k novým technológiám a majú možnosť sa s nimi zoznámiť, začať ich aktívne využívať a pochopiť ich nevyhnutnosť v dnešnej dobe.

4.6 Zabezpečenie

Riadenie a správa prístupu do bezdrôtovej siete sú dôležité na jej úspešné fungovanie. Vďaka pokroku poskytuje technológia Wi-Fi silné zabezpečenie a ochranu, takže dáta sú ľahko dostupné len tým ľuďom, ktorí majú povolený prístup. Prístupové body spoločnosti Cisco sú známe svojou oceňovanou implementáciou štandardizovaných a rozšírených možností dôkladného zabezpečenia.

Metódu zabezpečenia bola zvolená WPA-PSK. Treba mať na zreteli, že sa jedná o centrum pre deti bez potrebnej infraštruktúry (radius server) na použitie enterprise módu. Pre spätnú podporu starších notebookov a počítačov nebolo možné použiť WPA2 (AES šifru).

Pre dostatočnú bezpečnosť bola zmenená defaultná „WaveLAN Network“ hodnota SSID. Na hodnotu, ktorá nenesie žiadnu súvislosť s názvom centra.

Pretože centrum si vedie zoznamy detí, ktoré navštevujú toto centrum, tým pádom je možné zostaviť zoznam autorizovaných MAC adries a neznáme adresy sú automaticky odmietnuté.

4.7 Ekonomické zhodnotenie

Konečná suma za zariadenia použité pri vytvorení bezdrôtovej siete činila 2564,97 €. Táto cena je pre fyzickú osobu, alebo domácnosť neprípustná ale pre organizáciu, ktorá získava financie od svojich sponzorov a dotácií je celkovo priateľská. Pretože sa jedná o kvalitné priam najkvalitnejšie zariadenia v súčasnosti, ktoré skoro dokonale zabezpečujú sieť a dáta v nej. Aj keď sa jedná len o centrum pre deti vo voľnom čase, dáta sú niekedy veľmi dôležité a majú nevyčísliteľnú hodnotu.

4.7.1 Náklady na výstavbu

Tabuľka 9. Finančné náklady na realizáciu (Zdroj vlastný)

Zariadenie	**Cena za 1Ks**	**Množstvo**	**Cena celkom**
Cisco Wireless LAN Controller 2106	382,69 €	1	382,69 €
Cisco 1000 Series AP	1 091,14 €	2	2182,28 €
		Finálna cena	**2564,97 €**

4.7.2 Prínosy riešenia pri vybudovaní bezdrôtovej siete

- Mobilita;
- Flexibilita;
- Úspora nákladov;
- Prispôsobiteľnosť a rozšíriteľnosť;
- Široké pokrytie;
- Výkon siete;
- Zabezpečenie.

Mobilita

Najzrejmejším prínosom bezdrôtovej siete je sloboda pohybu. S notebookom alebo PDA je možné byť pripojený a voľne sa pohybovať. Zamestnanci sa na cestách môžu ľahko pripojiť k sieti svojej kancelárii, bez toho aby museli hľadať vhodný ethernetový port. Pracovníci, ktorý sa často pohybujú po kancelárii alebo pracovisku v rámci svojej pracovnej náplne, si môžu vziať zo sebou notebook alebo PDA a mať stále prístup k elektronickej pošte a databázam. (2)

Flexibilita

Bezdrôtové počítače sa môžu dostať tam, kde sa káblom zapojené počítače nedostanú. Je možné ľahko premiestňovať svoje notebooky, ale bezdrôtová sieť taktiež umožní umiestniť stolný počítač v mieste, kde nie je možné viesť káble a podľa svojho uváženia tieto počítače premiestňovať bez ohľadu na to, kde sú sieťové pripojenia k dispozícií. Bezdrôtová sieť taktiež uľahčuje prístup na podnikovú sieť hosťom alebo deťom, ktorý si zo sebou priniesli svoje notebooky a potrebujú dočasný prístup na sieť či na internet. (2)

Úspora nákladov

Natiahnutie káblov často predstavuje pre podniky významné náklady, alebo je náročné na ľudskú prácu. Návrh a inštalácia káblových sietí môže byť taktiež dosť nákladná. Vybudovanie bezdrôtovej siete by mohlo stáť viac než káblové siete, pretože je potrebné kúpiť bezdrôtové sieťové adaptéry pre každý počítač taktiež aj bezdrôtový prístupový bod. Náklady na bezdrôtovú sieť sú v tomto zmysle vyššie, pri stolných počítačoch bez zariadení na bezdrôtový prenos. Ale väčšina dnešných počítačov a mobilov obsahuje tieto zariadenia, ktorými je možné sa pripojiť. (2)

Prispôsobiteľnosť a Rozšíriteľnosť

Je schopnosť rozšírenia siete po jej počiatočnej inštalácii. V tejto sfére je táto schopnosť veľmi dôležitá pre efektívne riadenie rastu zariadení. Nie je potreba, pripájať ďalšiu infraštruktúru. So svojím notebookom, vybaveným zariadením pre bezdrôtovú komunikáciu sa nový pracovník môže pripojiť v momente bez zbytočných komplikácií. Tieto bezdrôtové prístupové body môžu podporovať až 150 užívateľov v závislosti na výkone a parametroch daného zariadenia. (2)

V káblovej sieti je potrebné pre každé sieťové zariadenie ethernetové porty na rozbočovači (Hub alebo Switch). Na podporu 30 užívateľov je potrebné napr. štyri 8-portové ethernetové rozbočovače a je potreba pridávať nový vždy, keď dôjde k rastu užívateľov. (2)

Prístupové body pracujú na úlohách pokrytia a základných služieb na podporu mobility samostatne. Pri rozšírených aplikáciách a centralizovanej správe viacerých prístupových bodoch spolupracujú s radičmi Cisco Wireless LAN.

Široké pokrytie

Použité prístupové body od spoločnosti Cisco patria v súčasnosti medzi najkvalitnejšie zariadenia. Poskytujú kvalitné, rozsiahle pokrytie bezdrôtového signálu.

Výkon siete

Vysokokapacitné duálne vysielače poskytujú flexibilitu, kapacitu a výkon na podporu širokého spektra mobilných aplikácií, ako napríklad prístupu s oprávneniami hosťa alebo hlasových služieb prostredníctvom bezdrôtovej siete LAN.

Záver

Celkové zhodnotenie bezdrôtových sietí vedie k tomu, že táto problematika prináša či už administrátorom alebo užívateľom množstvo výhod, ale samozrejme aj pár nevýhod. Vďaka inštitútu IEEE a WiFi aliancií, ktoré úzko spolupracujú a podieľajú sa na nových doplnkoch pre tieto siete sa eliminujú hlavné ich nedostatky.

Hlavnými prínosmi sú ľahká implementácia a vysoký komfort pre užívateľov či už z hľadiska rýchleho pripojenia alebo mobility, hlavne v dnešnej dobe, kedy sa využívajú bezdrôtové technológie skoro v každom sektore. Pre domáce pohodlie sú zariadenia veľmi často nakonfigurované tak, aby pri ich „vybalení“, hneď pracovali bez zbytočných nastavovaní. Tým pádom odpadá množstvo bezpečnostných prvkov, ktoré túto sieť chránia.

Hoci štandard WPA je relatívne kvalitné zabezpečenie a WPA2 dokonca najkvalitnejšia alternatíva zabezpečenia, nedá sa očakávať že bez ďalších metód zabezpečení bude táto sieť plne zabezpečená voči napadnutiu. Pokiaľ je možné využiť tieto zabezpečenia a klady, tak by sa mali plne využiť a odstrániť. V tom prípade sa takáto sieť stáva veľkým prínosom.

Zariadenia použité z návrhu sú pre domácnosti veľmi nákladné, ale s postupom času je možné predpokladať, že sa vplyvom konkurencie tieto zariadenia stanú prístupné napríklad pre obyčajný návrh domácej siete.

Zoznam použitej literatúry

(1) BARKEN,Lee. Wi-Fi: *jak zabezpečit bezdrátovou síť*. 1.vyd. Brno : Computer Press, 2004. 174 s. ISBN 80-251-0346-3.

(2) BRISBIN, Shelly. *Wi-fi: postavte si svou vlastní wi-fi síť*. 1.vyd. Praha : Neocortex, 2003. 248 s. ISBN 80-86330-13-3.

(3) PUŽMANOVA, Rita. *Bezpečnost bezdrátové komunikace : Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G*. Brno : Computer Press, 2005. 184 s. ISBN 80-251-0791-4.

(4) ZANDL,Patrick. *Bezdrátové sítě WiFi : praktický průvodce*. 1.vyd. Brno : Computer Press, 2003. 190 s. ISBN 80-7226-632-2.

Zoznam použitých webových zdrojov

(5) MAC adresa. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 19. január 2006, last modified on 12. apríl 2011 [cit. 2011-05-16]. Dostupné z WWW: <http://sk.wikipedia.org/wiki/MAC_adresa>.

(6) NOSKA, Martin . *Průzkum: Téměř dvě třetiny organizací zanedbává bezpečnost bezdrátových sítí.* [online]. 2009 [cit. 2011-05-18]. Dostupné z WWW: <http://computerworld.cz/aktuality/pruzkum-temer-dve-tretiny-organizaci-zanedbava-bezpecnost-bezdratovych-siti-3820>.

(7) SOVA, Martin . *Jak se prodává bezdrátová síť aneb několik rad, které se menším sítím budou hodit*. [online]. 2006 [cit. 2011-05-18]. Dostupné z WWW: <http://www.internetprovsechny.cz/jak-se-prodava-bezdratova-sit-aneb-nekolik-rad-ktere-se-mensim-sitim-budou-hodit/>.

(8) TŘÍSKA, Ing. Jaromír. Bezdrôtové siete : Bezdrôtové siete LAN – IEEE 802.11. In *Bezdrotove_siete.pdf* [online]. SPŠE : Piešťany, 2008 [cit. 2011-05-16]. Dostupné z WWW: <http://www.spsepn.edu.sk/skola/pk_info/studium/ucebtext/ele/siete/bezdrotove_siete.pdf>.

(9) VOKÁL, Aleš . *Bezdrátové sítě zažívají růst.* [online]. 2003 [cit. 2011-05-18]. Dostupné z WWW: <http://www.profit.cz/clanek/bezdratove-site-zazivaji-rust.aspx>.

(10) *Wi-fi.unas.cz* [online]. 2010 [cit. 2011-05-16]. Wi-Fi Wireless LAN. Dostupné z WWW: <http://wi-fi.unas.cz/>.

(11) *Wi-fi.unas.cz* [online]. 2010 [cit. 2011-05-16]. SSID. Dostupné z WWW: <http://wi-fi.unas.cz/ssid.php>.

(12) *Wi-fi.unas.cz* [online]. 2010 [cit. 2011-05-16]. WEP. Dostupné z WWW: < http://wi-fi.unas.cz/wep.php>.

(13) *Wi-fi.unas.cz* [online]. 2010 [cit. 2011-05-16]. WPA2. Dostupné z WWW: < http://wi-fi.unas.cz/wpa2.php>.

(14) ZRNÍK, Jakub . *Bezdrat.webnode.cz : modulace* [online]. 2008 [cit. 2011-05-16]. Bezdrátové sítě. Dostupné z WWW: <http://bezdrat.webnode.cz/modulace/>.

Zoznam skratiek

AES	Advanced Encryption Standard
AES	Advanced Encryption Standard
AP	Access Point
ASCII	American Standard Code for Information Interchange
BPSK	Binary Phase Shift Keying
BSS	Basic Service Set
CCK	Complementary Code Keying
CCM	Cipher Block Chaining Message Authentication Code
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CDMA	Code-Division Multiple Access
CRC	Cyclic Redundancy Check
DBPSK	Differential Binary Phase Shift Keying
DECT	Digital Enhanced Cordless Telecommunications
DQPSK	Differential Quadrature Phase Shift Keying
DS	Distribučný Systém
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol over LANs
ESS	Extended Service Set
FHSS	Frequency-Hopping Spread Spectrum
GSM	Global System for Mobile Communications
CHAP	Challenge Handshake Authentication Protocol
IAPP	Inter-Access Point Protocol
IEEE	Institute of Electrical and Electronics Engineers
IR	Infra Red

ISM	Industrial Scientific Medical
IV	Initialization Vector
LAN	Local Area Network
LEAP	Lightweight Extensible Authentication Protocol
MAC	Media Access Control
MD5	Message Digest
MIC	Message Integrity Check
MIMO	Multiple-Input Multiple-Output
NAS	Network Access Server
OFDM	Orthogonal Frequency-Division Multiplexing
PEAP	Protected Extensible Authentication Protocol
PKI	Public Key Infrastructure
PMK	Pairwise Master Key
PPP LCP	Point-to-Point Protocol Link Control Protocol
PRNG	Pseudo-Random Number Generator
QAM	Quadrature amplitude modulation
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RSN	Robust Security Network
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Level Security
TTLS	Tunneled Transport Layer Security
UDP	User Datagram Protocol
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity
WPA	Wi-Fi Protected Access

Zoznam obrázkov

Zoznam tabuliek