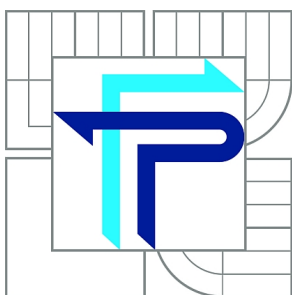




VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

BEZDRÁTOVÉ SÍTE VE FIREMNÍM PROSTŘEDÍ

WIRELESS NETWORKS IN CORPORATE ENVIRONMENT

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

TOMÁŠ SVITANA

VEDOUCÍ PRÁCE
SUPERVISOR

doc. Ing. MILOŠ KOCH, CSc.

BRNO 2010

Abstrakt

Obsahom mojej bakalárskej práce sú bezdrôtové siete. Za všeobecným úvodom zameraným na terminológiu, používané protokoly, štandardy, topológiu ako aj na samotné zabezpečenie sa nachádza konkrétny návrh a implementácia bezdrôtovej technológie do firemného prostredia.

Firma poskytuje voľne prístupnú hotelovú Wi-Fi sieť na strediskách a zároveň pre interné účely požaduje kvalitne zabezpečený bezdrôtový prenos dát.

Abstract

Purpose of my bachelor's thesis is wireless networks. The general introduction focused on basic terminology, most used protocols, standards, and topology and also network security is followed by specific draft and implementation of wireless technology into corporate environment.

Company provides free accessible hotel Wi-Fi network on main departments and also for internal use requires high level secured wireless transfer of data.

Klíčové slová

Wi-Fi, bezdrôtová sieť, WLAN, WEP, WPA, WPA2, IEEE 802.11, SSID, zabezpečenie, 4. generácia WLAN.

Keywords

Wi-Fi, wireless network, WLAN, WEP, WPA, WPA2, IEEE 802.11, SSID, security, 4th generation WLAN.

Bibliografická citácia

SVITANA, T. *Bezdrátové síte ve firemním prostředí*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2010. 52 s. Vedúci bakalárskej práce doc. Ing. Miloš Koch, CSc.

Čestné prehlásenie

Prehlasujem, že predložená bakalárska práca je pôvodná a spracoval som ju samostatne. Prehlasujem, že citácie použitých prameňov je úplná, že som vo svojej práci neporušil autorské práva (v zmysle Zákona č. 121/2000 Sb., o práve autorskom a o právach súvisiacich s právom autorským).

V Brne dňa

.....

Tomáš Svitana

PodĎakovanie

Rád by som poďakoval vedúcemu mojej bakalárskej práce, doc. Ing. Milošovi Kochovi CSc. za jeho prínosné rady a metodickú pomoc, ktoré ma nasmerovali k vypracovaniu tohto dokumentu.

OBSAH

Úvod.....	8
1 Vymedzenie problému a ciele práce.....	9
2 Teoretické východiská.....	10
2.1 Úvod do bezdrôtových sietí.....	10
2.1.1 Rádiový signál.....	11
2.1.2 Optický signál.....	12
2.2 IEEE 802.....	13
2.3 Referenčný model OSI.....	14
2.4 IEEE 802.11.....	15
2.4.1 Problémy IEEE 802.11.....	15
2.4.2 802.11b.....	17
2.4.3 802.11a.....	17
2.4.4 802.11g.....	17
2.4.5 802.11n.....	18
2.4.6 Doplnkové normy 802.11.....	19
2.4.7 Výhľad do budúcnosti.....	20
2.5 Topológia WLAN.....	23
2.5.1 Ad-hoc.....	23
2.5.2 Infraštruktúra.....	24
2.6 Hardware pre WLAN.....	25
2.6.1 Aktívne prvky.....	25
2.6.2 Antény.....	26
2.7 Ochranné prvky a metódy útokov na WLAN.....	28
2.7.1 Primárne zabezpečenie.....	28
2.7.2 Hide SSID.....	29
2.7.3 Filtrovanie adres.....	29
2.7.4 WEP.....	30
2.7.5 WPA.....	30
2.7.6 WPA2.....	31
2.7.7 Autentizácia 802.1X.....	32

3	Analýza problému a súčasná situácia	33
3.1	Firemná WLAN v ohrození	34
3.2	Aktuálny stav	35
4	Vlastný návrh riešenia	36
4.1	Predstavenie spoločnosti	36
4.2	Pôdorys hlavného podlažia hotela.....	37
4.3	Priblíženie podstaty riešenia	38
4.4	Výber vhodného hardvéru.....	38
4.4.1	EXSW – 1200	38
4.4.2	EXRP – 40	40
4.5	Rozmiestnenie hardvéru.....	41
4.5.1	Poloha AP v administratívnej zóne.....	41
4.5.2	Poloha AP v hotelovej zóne.....	42
4.6	Konfigurácia siete a zariadení.....	43
4.6.1	Blanket Zamestnanci_International	43
4.6.2	Blanket Hot-Spot_International.....	43
4.6.3	Blanket Administrácia	44
4.6.4	Ostatné periférie.....	45
4.7	Kalkulácia nákladov	46
	Záver	48
	Zoznam použitej literatúry.....	49
	Zoznam obrázkov	51
	Zoznam tabuliek	51
	Zoznam príloh.....	52

ÚVOD

V dnešnej dobe pozorujeme rozmach internetu v strednej Európe. Priamoúmerne narastá aj počet internetových providerov, ktorý ponúkajú rôzne druhy pripojení do siete internet. Najstaršie a najpoužívanejšie je pripojenie pomocou metalických vodičov rôznych kategórií. Modernou technológiou využívanou predovšetkým v minulosti na výstavbu barebone siete avšak v súčasnosti prístupnej i koncovým užívateľom je optická kabeľáž zložená zo štruktúry optických vlákien schopných vysokorýchlostného prenosu dát. Bezdrôtová technológia je vo svojej podstate nadstavbou metalických a optických sietí, ktoré vždy tvoria jej základ.

Počínajúc mobilnými telefónmi, cez predaj notebookov až po cenovo prijateľné routery a prístupové body, prešli bezdrôtové systémy prudkým a razantným vývojom. Vďaka rýchlym reakciám na požiadavky užívateľov a firiem v oblasti zdokonaľovania a rozširovania sady štandardov pre bezdrôtové lokálne siete, pozorujeme od roku 2006 ich rozmach najmä u bežných používateľov. Heslom nového tisícročia sa preto stala mobilita. Synonymom tohto slova na poli informačných technológií pre bežných používateľov sú práve výkonovo neustále rastúce notebooky v spojení s Wi-Fi¹, ktorých predaj v pomere k stolovým PC neustále rastie a posilňuje.

Samotná výhoda WLAN, voľnosť bezkáblového pripojenia, a jej masové rozšírenie až k užívateľom – začiatočnikom, otvára závažnú otázku problematiky bezpečnosti siete a ochrany pred zneužitím. Tejto a mnohým iným zaujímavým skutočnostiam sa budeme venovať v jednej z nasledujúcich kapitol.

¹ Skratka významu *Wireless Fidelity*, čo v preklade znamená *bezdrôtová vernosť*. Ide o alianciu, ktorá certifikuje vzájomnú kompatibilitu zariadení pracujúcich na štandarde IEEE 802.11.

1 VYMEDZENIE PROBLÉMU A CIELE PRÁCE

Problém bezdrôtových sietí vo firemnom prostredí spočíva najmä v ich zabezpečení na rôznych vrstvách sieťového protokolu. Softvérová bezpečnosť je však len ďalším krokom nasledujúcim po hardvérovom zaistení zraniteľných bodov systému. V protiklade dostatočne chránenej bezdrôtovej siete je voľne prístupná sieť tzv. Hot Spot ako služba pre hostí, ktorá poskytuje pripojenie do internetu. Primárnou úlohou je vytvorenie firemnej bezdrôtovej siete a Hot Spotu.

Cieľom teoretickej časti mojej bakalárskej práce je priblíženie bezdrôtových sietí, ich vývoj a špecifikácia, technologické pozadie a široko diskutovaná téma bezpečnosti WLAN.

V konkrétnom návrhu riešenia sa budeme venovať už zmienenej tvorbe firemnej bezdrôtovej siete a verejného prístupového bodu Hot Spot. Prístupné a moderné riešenie vychádza z použitia technológie bezdrôtových sietí štvrtej generácie. Za dosiahnutie cieľa považujeme vybudovanie jednoduchej, účelnej a dobre zabezpečenej bezdrôtovej siete. Určite v nasledujúcich kapitolách pochopíme, že pojem „dobre zabezpečená bezdrôtová sieť“ je vlastne utopický.

2 TEORETICKÉ VÝCHODISKÁ

2.1 Úvod do bezdrôtových sietí

Vo všeobecnosti bezdrôtová sieť je chápaná ako sieť, v ktorej prebieha komunikácia zariadení bez nutnosti použitia alebo pripojenia k metalickým a optickým vodičom.

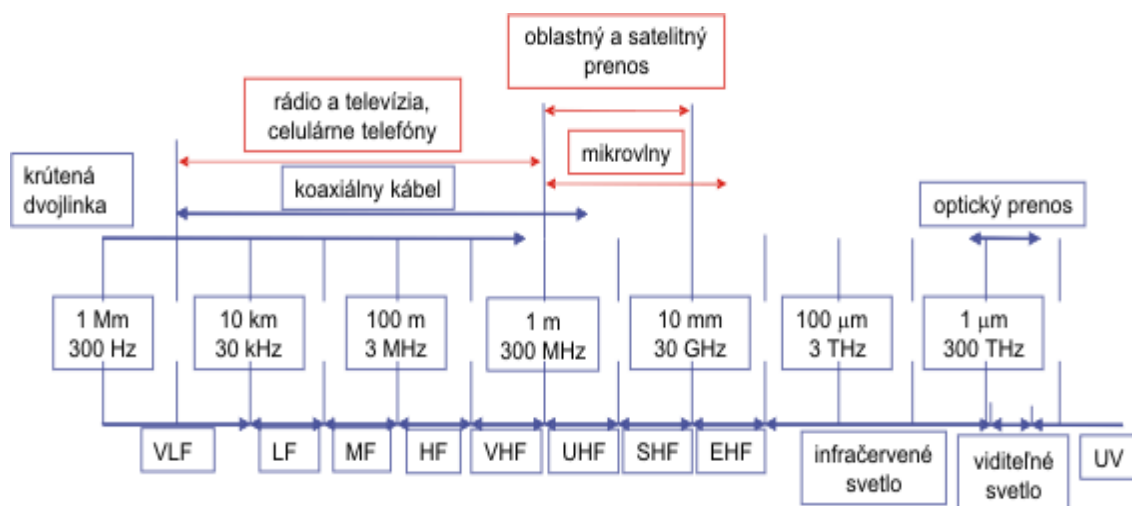
Vedúcim faktorom rozmachu bezdrôtových sietí je množstvo ich výhod. Najvýraznejším prvkom skupiny výhod je nepochybne *mobilita*, ktorá umožňuje voľne presúvať zariadenia kdekoľvek v oblasti dosahu rádiového signálu siete. *Flexibilita* ako ďalší prvok predstavuje možnosť nekonečnej variability umiestnenia zariadení v oblasti dosahu a to hlavne bez potreby inštalácie kabeláže a jej premiestnenia. Staršie objekty a domy nie sú stavané s ohľadom na potrebu kabeláže (inštaláčne šachty), preto je u nich možnosť bezdrôtového pokrytia pomerne často využívaná. Výrazný ekonomický faktor ako *úspora nákladov* má svoje kľúčové postavenie pri výbere používanej technológie prenosu dát. Inštalácia metalickej sieťovej kabeláže pre všetky koncové zariadenia je finančne náročnejšia než vybudovanie bezdrôtovej siete. Moderné zariadenia disponujú okrem vstavaného ethernetového portu aj bezdrôtovým adaptérom, preto sa náklady v porovnaní s predošlými rokmi znížili pri ohľade na potrebné do vybavenie bezdrôtovým adaptérom. Progresívne spoločnosti požadujú technológie, ktoré im umožnia v prípade rozšírenia pružne modifikovať aj sieť. *Prispôsobiteľnosť* metalickej siete so sebou prináša vysoké náklady na nové aktívne prvky a časovú náročnosť. Bezdrôtové siete naopak umožňujú okamžité vytvorenie nového prístupu k sieti s minimálnymi nákladmi a nulovou časovou náročnosťou.(1)

Pre správne poňatie spomenutej terminológie musíme zaradiť všetky bezdrôtové siete pod jednu veľkú skupinu, do ktorej patria všetky systémy založené na báze prenosu dát vzduchom z jedného bodu do druhého.

2.1.1 Rádiový signál

Najznámejšími prvkami v oblasti šírenia dát rádiovým signálom sú v jednotlivých pásmach (Obrázok 2.1):

- *Veľmi vysokej frekvencie (VHF)* s rozsahom 30 – 300 Mhz
 - FM rádiové vysielanie (87.5-108MHz),
 - televízne vysielanie.
- *Ultra vysokej frekvencie (UHF)* o rozsahu 300 – 3000 MHz
 - televízne vysielanie,
 - mobilné telefóny so systémom NMT (450 MHz a 900 MHz),
 - jeho nástupca GSM² s frekvenciami 900 MHz a 1800 MHz,
 - mobilné siete 3G na frekvencii 2100 MHz,
 - pre nás zaujímavé bezdrôtové lokálne siete WLAN na frekvencii 2,4 GHz.
- *Super vysokej frekvencie (SHF)* pri rozsahu 3 – 30 GHz
 - mikrovlnné technológie 26 GHz,
 - bezdrôtové lokálne siete WLAN na frekvencii 5 GHz.



Obrázok 2.1 Grafické znázornenie rozdelenia frekvencií (2)

² Skratka významu *Global System For Mobile Communications*, v preklade *globálny systém pre mobilnú komunikáciu*

2.1.2 Optický signál

Bezdrôtové optické siete používajú pre prenosy vzduchom neviditeľné svetelné lúče infračerveného spektra o vlnovej dĺžke 1550 nm a 800 nm. Združujú v sebe rýchlosť prenosu optického vlákna s výhodami bezdrôtovej technológie. Technológia FSO (Free Space Optics) ponúka rýchlosti prenosu od 100 Mbit/s až po doposiaľ možných 2,7 Gbit/s. Aktuálne trendy v tejto oblasti smerujú k využívaniu LED technológie, ktorá minimalizuje negatívne vplyvy počasia a poskytuje 99,995 percentnú spoľahlivosť.

Výhodami uvedenej technológie je:

- vysoká rýchlosť prenosu,
- prenos na veľké vzdialenosti, ktorý sa štandardne pohybuje v stovkách metrov a niektorí výrobcovia dokonca garantujú dosah 4 km,
- nízke náklady na zriadenie,
- vysoká bezpečnosť,
- flexibilita inštalácie.

Radu výhod z veľkej miery zatieňuje súbor nevýhod. Medzi najvýraznejšie patria:

- nutnosť priamej viditeľnosti vysielača a prijímača (akákoľvek prekážka, či už trvalá alebo dočasná, spôsobí prerušenie spojenia a prenosu dát),
- atmosférické zmeny, najmä hmla a hustý dážď (napríklad pri ľahkej hmle a silnom daždi je útlm cca 10dB/km).

Každý problém má zväčša aj svoje riešenie. V tomto prípade sa používajú záložné systémy pre prípad zlyhania FSO. Hybridný systém, ktorý pozostáva z optického prenosu FSO a zároveň disponuje automatickým záložným rádiovým spojom, je riešením na uvedené problémy optického bezdrôtového prenosu. (3)

2.2 IEEE 802

Ide o rodinu štandardov pre lokálne a metropolitné siete, ktoré vypracovala medzinárodná nezisková organizácia IEEE³ so sídlom v New Yorku. Jednotlivé štandardy z celého spektra pokrývajú dostatočne požiadavky LAN/MAN sietí. (4) Najznámejšie sú štandardy:

- *IEEE 802.3* – ethernet (LAN),
- *IEEE 802.3af* – POE⁴ napájanie sieťových zariadení prostredníctvom ethernetového káblu
- *IEEE 802.11* – bezdrôtové lokálne siete (WLAN),
- *IEEE 802.15* – bezdrôtové osobné siete (WPAN).

³ Skratka významu *Institute of Electrical and Electronics Engineers*, v preklade *Inštitút elektrotechnických a elektronických inžinierov*.

⁴ Skratka významu *Power Over Ethernet*, v preklade napájanie cez ethernetový kábel.

2.3 Referenčný model OSI

Tak ako všetky siete, aj WLAN sú vo svojej podstate postavené na referenčnom modeli prepojenia otvorených systémov OSI⁵ (Obrázok 2.2). Tento model je rámec siedmich vrstiev, ktoré popisujú štruktúru a priebeh komunikácie od najnižšej – fyzickej vrstvy, až po aplikačnú vrstvu. Typickým pre model je jeho hierarchické usporiadanie. Napríklad základné sieťové funkcie, ako dekódovanie rádiového signálu, prebieha na nižších vrstvách. Naopak vyššie vrstvy riadia spôsob, akým sú transakcie vykonávané. Dôležitá je informácia, že nie všetky sieťové normy a protokoly musia využívať všetky vrstvy OSI.



Obrázok 2.2 Referenčný model OSI

Všetky normy IEEE 802 pracujú na fyzickej vrstve a na spojovej vrstve. To zahŕňa špecifikácie IEEE 802.3, 802.5 (kruhová sieť) a 802.11. Protokoly na vyšších vrstvách modelu OSI ako napríklad TCP/IP, NetBIOS a iné sú úplne nezávislé na nižších vrstvách. Používajú ich ako platformu, na ktorej bežia.

Spojová vrstva je štandardom IEEE 802 rozdelená na 2 podvrstvy a to *podvrstva riadenia logického spoja LLC* (IEEE 802.2), ktorá vykonáva zapúzdrenie paketov prijímaných od nižších vrstiev a *podvrstva riadenia prístupu k médiu* (Media Access Control). (1)

⁵ Skratka významu *Open Systems Interconnection*, v preklade *Prepojenie otvorených systémov*.

2.4 IEEE 802.11

Jeden z prvých komerčných WLAN systémov vyvinula spoločnosť Motorola pod názvom *ALTAIR*. Poskytoval len nízke prenosové rýchlosti a bol náchylný k interferenciám rádiového prenosu. Ako nástupcu inicioval roku 1990 inštitút IEEE projekt 802.11, zameraný na vývoj špecifikácií pre vrstvu riadenia prístupu (MAC) a fyzickú vrstvu (PHY) pre bezdrôtovú konektivitu pevne zabudovaných, prenosných a pohyblivých staníc v oblasti. Sedem rokov neskôr, presnejšie 27. júna 1997, schválil inštitút práve IEEE 802.11 ako medzinárodný štandard pre WLAN.

Základné parametre štandardu IEEE 802.11, jeho prvej verzie, boli používanie 2,4 GHz pásma a prenosová rýchlosť 1 – 2 Mbps⁶. V súčasnosti sa už táto verzia nepoužíva. Bola nahradená výkonnejšími štandardmi IEEE 802.11b/g/n.

Pásmo 2,4 GHz bolo vymedzené americkým regulátorom FCC, aj európskym regulátorom ETSI ako voľné pásmo pre ISM⁷. Na území Českej republiky spravuje vysielacie spektrum Český telekomunikačný úrad. Okrem rozdelenia frekvencií a ich správu a kontrolu vykonáva ČTU aj reguláciu ISM pásma a to hlavne obmedzením vyžarovacieho výkonu zariadení a používaním práve jednej z troch technológií rozprestretého spektra. (5)

Rozprestrené spektrum členíme:

- rozprestrené spektrum v priamej postupnosti (DSSS)
- rozprestrené spektrum s preskakovaním medzi frekvenciami (FHSS),
- ortogonálny frekvenčný multiplex (OFDM).

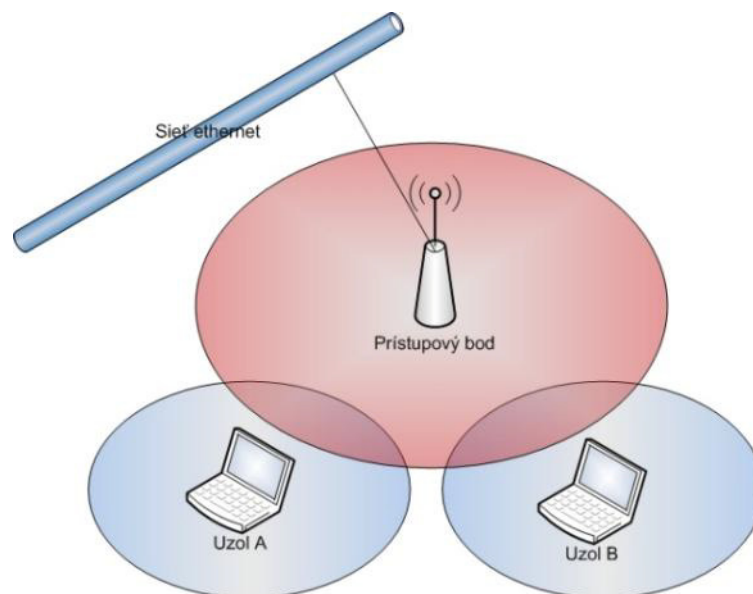
2.4.1 Problémy IEEE 802.11

S prihliadnutím na rozdiely v rámci kontinentov je z globálneho hľadiska možné vnímať uvoľnenie časti frekvenčného pásma na voľné použitie ako nie práve výhodný krok. Súčasná situácia ukazuje prudko rastúcu tendenciu používania zariadení na bezdrôtový prenos so štandardmi 802.11b/g/n, pričom sa tým stáva pásmo 2,4 GHz takmer nepoužiteľné a to v prvom rade vo vyspelých a husto osídlených oblastiach, kde sa bytové WLAN stretávajú s korporátnymi riešeniami o vysokom výkone.

⁶ Skratka významu *Megabits per second*, v preklade *Megabitov za sekundu*.

⁷ Skratka významu *Industrial, Scientific and Medical*, v preklade *Priemyselné, vedecké a medicínske pásmo*.

Pôvodne bolo o štandarde IEEE 802.11 uvažované pre použitie v interiéri nahrádzajúce ethernetové siete. Tomu primeraný je aj prístup, akým sa WLAN dokážu vyrovnáť s kolíziami. Systém predchádzajúci kolíziám CSMA/CA používa potvrdzovanie RTS/CTS (RequestToSend/ClearToSend) a to z dôvodu eliminácie problému so *skrytým uzlom* (Obrázok 2.3). Spomínaný problém je možné opísať ako stav, vyskytujúci sa pri používaní WLAN v rozľahlých objektoch alebo exteriéri spôsobom Point-to-Multipoint (jeden AP⁸ obsluhuje viacero zariadení). Spôsobuje ho vysielanie klientskych staníc súbežne v domienke, že je priestor k prenosu voľný, kedy dochádza k zahlteniu AP. Aj napriek kombinácii CSMA/CA a RTS/CTS znamená skrytý uzol zníženie priepustnosti siete a nárast strát paketov. Riešenie môže byť hardvérové alebo softvérové. Hardvérové je finančne náročnejšie, lebo vyžaduje nahradenie systémom point-to-point (z AP do jedného zariadenia). Softvérové riešenie je možné, ak má AP konfigurovateľný RTS/CTS treshold (prahová hranica RTS/CTS) a veľkosť fragmentov na ktoré sa delia rámce. Na presné nastavenie spomenutých hodnôt nájdeme mnoho voľne dostupných programov.



Obrázok 2.3 Problém skrytého uzlu

⁸ Skratka významu *Access Point*, v preklade prístupový bod.

2.4.2 802.11b

Norma 802.11b, ratifikovaná v roku 1999, je aktualizovanou a vylepšenou verziou pôvodnej normy. Maximálna priepustnosť je stanovená na 11 Mbps a používa CSMA/CA prístup k médiu podľa IEEE 802.11. Reálna priepustnosť sa však pohybuje na hranici 6 Mbps. Modulačná technológia DSSS je taktiež prevzatá z pôvodného štandardu. Dosah v interiéri je približne 30 metrov a v exteriéri do 100 metrov. S navýšením vzdialenosti medzi vysielačom a prijímačom klesá úmerne aj priepustnosť z maxima 11 Mbps až na 1 Mbps.

Zariadenia vychádzajúce zo štandardu 802.11b pomerne rýchlo zaplnili trh. Dôvodom bol pokles ceny zariadení, navýšenie výkonu na postačujúcu úroveň (v roku 1999) a pre výrobcov jednoduchý zásah do chipsetu zariadenia kvôli softvérovému rozšíreniu.

Popri hlavnom štandarde ponúkali výrobcovia čipov WLAN aj proprietárne štandardy. Ich vlastnosťou je kompatibilita iba v rámci jednej produktovej rodiny toho istého výrobcu. Pri štandarde IEEE 802.11b prišla s technológiou štvornásobného zvýšenia rýchlosti spoločnosť Texas Instruments a ich produkty niesli označenie 802.11b+. Avšak z dôvodu použitia rozšírenej technológie len v zariadeniach Texas Instruments nenašla modifikácia uplatnenie na trhu.(6)

2.4.3 802.11a

IEEE 802.11a, schválená tesne po norme 802.11b pracuje v pásme 5 GHz (5,15 - 5,825 GHz). s priepustnosťou do 54 Mbps. Používa metódu rozprestretého spektra OFDM. Hlavným pozitívom je široké pásmo s dostatočným rozsahom medzi kanálmi. Negatívom sú vyššie náklady pri obstaraní a menšia priepustnosť cez pevné prekážky. Nie je tu kompatibilita so IEEE 802.11b, ale zároveň nedochádza pri koexistencii k rušeniu.

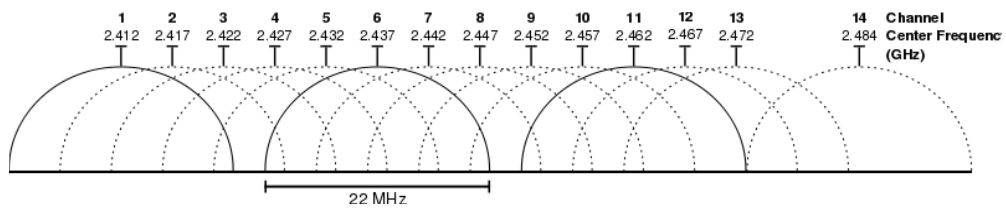
Tento štandard je používaný hlavne vo väčšom firemnom prostredí než tomu je v domácnostiach a malých firmách.(1)

2.4.4 802.11g

Tretia sieťová norma IEEE 802.11g bola schválená v roku 2002. Podobne ako 802.11a používa rovnakú technológiu OFDM. Maximálna rýchlosť je 54 Mbps.

Frekvenčné pásmo je zhodné s 802.11b – 2,4 GHz a tiež je tu aj spätná kompatibilita s týmto štandardom a možnosť pracovať spoločne. Rada zariadení podporuje obidve normy súčasne.

Vysielané signály pri IEEE 802.11b/g sa nešíria presne, preto nie je možný prenos na všetkých 13 kanáloch súčasne. Bránia tomu malé rozstupy medzi jednotlivými kanálmi. Kvalitný prenos je zaručený ak medzi použitými kanálmi sú tri voľné kanály (Obrázok 2.4). Kanál 14 je povolený len v Japonsku. (6)

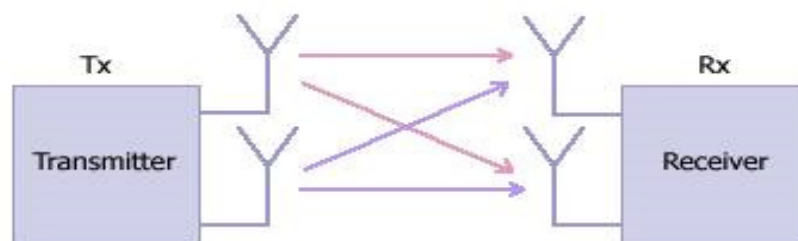


Obrázok 2.4 Rozloženie kanálov v pásme (7)

2.4.5 802.11n

Táto norma bola vyvíjaná od roku 2008 a oficiálne vydaná 29. októbra 2009. Za cieľ si kladie zvýšenie rýchlosti prenosu dát cez WLAN. Používa moduláciu OFDM a frekvencie 2,4 a 5 GHz. Samotná rýchlosť vzrástla z 54 Mbps na 600 Mbps (za určitých podmienok) pri použití štyroch dátových prúdov o šírke pásma 40 MHz a dosah pokrytia narástol až na 300 metrov v interiéri.

Majoritným dôvodom zvýšenia rýchlosti bola implementácia technológie MIMO⁹ (Obrázok 2.5). Jej princípom je použitie viacerých antén na oboch stranách, pomocou ktorých dosiahneme vyššie rýchlosti pri zachovaní štandardnej šírky pásma 20 MHz. (8)



Obrázok 2.5 MIMO technológia 2x2 (8)

⁹Skratka významu *Multiple-Input Multiple-Output*, v preklade *viac vstupov a viac výstupov*.

Každý štandard má svoje klady a zápory. IEEE 802.11n je oproti predchodcom finančne náročnejší na obstaranie zariadenia. Neodporúča sa používať MIMO technológiu v oblasti, kde súbežne pracuje aj IEEE 802.11b/g, pretože dochádza k prekryvaniu vysielačieho pásma. Taktiež je reálna priepustnosť 170 Mbps a pri používaní 802.11n v zarušenom pásme 2,4 GHz je ešte viac znižovaná. Ideálne rýchlosti sú dosahované v pásme 5 GHz pri použití MIMO 4X4 tj. štyroch antén.

Už od roku 2008 boli certifikované zariadenia na normu 802.11n – draft, ktorá predstavovala predchodcu finálnej verzie a mala za cieľ priblížiť novú technológiu bežným používateľom.

2.4.6 Doplnkové normy 802.11

Okrem základných WLAN noriem IEEE 802.11a/b/g/n vytvorila IEEE pracovné skupiny, ktorých poslaním je vytvorenie doplnujúcich noriem. Zvyčajne sú to prípady, kedy je potrebné opraviť starší protokol, eventuálne vývoj technológií požaduje nový doplnok normy.

- ❖ **802.11e** protokol Quality Of Service. Udeľuje niektorým dátovým paketom prioritu pred ostatnými paketmi. Je dôležitý najmä pre hlasovú komunikáciu cez internet a prúdové multimédiá.
- ❖ **802.11h** protokol Spectrum Manager doplňuje 802.11a. Rieši problém rušenia signálu WLAN na frekvencii 5 GHz inými zariadeniami ako radary a satelity.
- ❖ **802.11i** Enhanced Security. Vylepšený autentizačný a šifrovací algoritmus. Zavedenie WPA2.
- ❖ **802.11r** Roaming. Protokol umožňujúci bezstratový presun medzi AP.

Existuje približne dvadsať rôznych doplnkov noriem 802.11, ktoré majú menší či väčší efekt na protokoly. Vyššie spomenuté sú len najvýznamnejšie úpravy za posledné roky.

2.4.7 Výhľad do budúcnosti

Rýchle tempo vývoja informačných technológií a rastúci záujem o bezdrôtové technológie podnecuje ich vývoj, zvyšovanie rýchlosti prenosu dát a zväčšovanie dosahu sietí. Pri rozhl'ade do blízkej budúcnosti sa rysuje hneď niekoľko použiteľných a sľubných variant.

WirelessHD – štandard komerčne dostupný na trhu televízorov s vysokým rozlíšením (High Definition) od roku 2008. Za jeho vývojom stoja renomované značky ako Intel, Panasonic, LG, Samsung, Phillips, Sony, Toshiba a iné. Práve u spomínaných výrobcov nájdeme s určitosťou zariadenia podporujúce štandard WirelessHD, ktoré jednoducho identifikujeme pomocou prítomnosti loga (Obrázok 2.6).



Obrázok 2.6 Logo štandardu Wireless HD

Stačí si len predstaviť množstvo káblov, ktoré sprevádza zapojenie každého nového zariadenia čiernej techniky a okamžite oceníme prínos WirelessHD. Práve tento štandard má pri zachovaní vysokej kvality prenášaného nekomprimovaného obrazu a viackanálového zvuku namiesto kábového média (HDMI kábel) používať bezdrôtový prenos. Umožňuje vytvorenie WVAN (Wireless Video Area Network), čo je bezdrôtová sieť pre prenos videa. Maximálna rýchlosť prenosu sa pohybuje pri hodnote 26 Gbps, reálna je na hodnote 4 Gbps pri využívaní frekvencie 60 GHz. Nevýhodou vysokej frekvencie je silný útlm, čo obmedzuje dosah, na strane druhej však redukuje možnosti neautorizovaného pripojenia. (9)

WiGig - Aliancia Wireless Gigabit (Obrázok 2.7) pripravuje štandard, ktorý rovnako ako WirelessHD využíva pásmo 60 GHz a komunikuje na rýchlosti 6 Gbps. Spoločnosti podieľajúce sa na vývoji sú Atheros Communications, Broadcom, Dell, Intel, LG Electronics, Marvell International, MediaTek, Microsoft, NEC, Nokia, Panasonic, Samsung Electronics a Wilocity. Na rozdiel od WirelessHD má slúžiť pre všetky zariadenia a platformy. Vytvorí ekosystém vzájomných vzťahov, pričom nebudú nutné veľké zásahy do už existujúcich bezdrôtových zariadení po celom svete. (10)

V aktuálnej verzii 1.0 doplňuje a rozširuje vrstvu 802.11 MAC a je spätne kompatibilný so štandardom 802.11. Ponúka aj širokú škálu pokročilých bezpečnostných nastavení a správu napájania. Vývojári ďalej navrhujú, aby tento štandard bol predstavený pod označení 802.11AD

Dôležitým krokom pre WiGig bude jeho prijatie Wi-Fi alianciou, čím sa podstatne posilní postavenie na trhu pre nový štandard.



Obrázok 2.7 Logo Wireless Gigabit Alliance

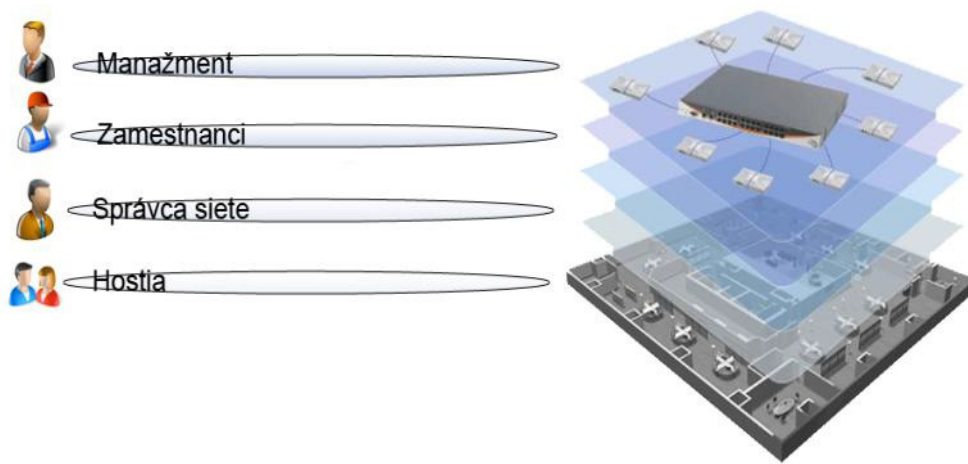
4.generácia Wi-Fi používa blanket architektúru s využitím tenkých AP vysielajúcich na rovnakom kanáli a tak vytvára celistvé pokrytie (blanket) s jednou unikátnou MAC adresou. Vďaka použitiu jedného kanálu pre celú sieť, je možné s jedným AP vytvoriť niekoľko fyzicky oddelených sietí. AP komunikujú s centrálnym prvkom, v ktorom sú zapojené a preto je tok dát synchronizovaný a prispôsobovaný aktuálnym podmienkam v reálnom čase.

Pri projektovaní umiestnenia AP už nemusíme prihliadať na možné rušenie. Naopak, platí tu heslo, čím viac AP, tým lepšie sieť funguje s väčším pokrytím. Vo svojej podstate klienti fyzicky komunikujú cez n-tý AP, ale logická cesta vedie cez centrálny prvok. Čo v prípade ak klient je v dosahu viacerých AP? Rozhodnutie preberá centrálny prvok, ktorý na základe intenzity signálu rozhodne.

Oproti tomu siete 3. generácie sú založené na bunkovej architektúre. To znamená, že každý AP je plne samostatný prístupový bod vysielajúci na jednom kanáli s unikátnou MAC adresou. Nevýhodou 3. generácie sú interferencie vnútri vlastnej siete spôsobené umiestnením viacerých AP, pričom sa vždy volí vhodný kanál z obmedzeného pásma 13 kanálov, ktoré však neposkytuje postačujúce rozstupy kanálov. Druhou slabinou je prechod zariadenia medzi jednotlivými AP, kde je nutné aby znovu prebehlo niekoľko zmien nastavenia. Aj napriek softvérovému riešeniu trvá prechod desiatok milisekúnd až niekoľko sekúnd. V praxi to spôsobuje výpadky služieb. Najnovší štandard 802.11n prináša so sebou ešte väčšie rušenie. Je to

spôsobené, ako už bolo spomenuté, použitím dvojnásobného pásma, čím znižuje počet použiteľných kanálov, ktoré sa vzájomne nerušia. (11)

Je možné prakticky využiť Wi-Fi 4. generácie na vytvorenie blanketov pre jednotlivé skupiny užívateľov (Obrázok 2.8). Jedná sa o novú technológiu, ktorej nevýhodou sú vyššie náklady pri výstavbe siete.



Obrázok 2.8 Možné využitie blanketov siete

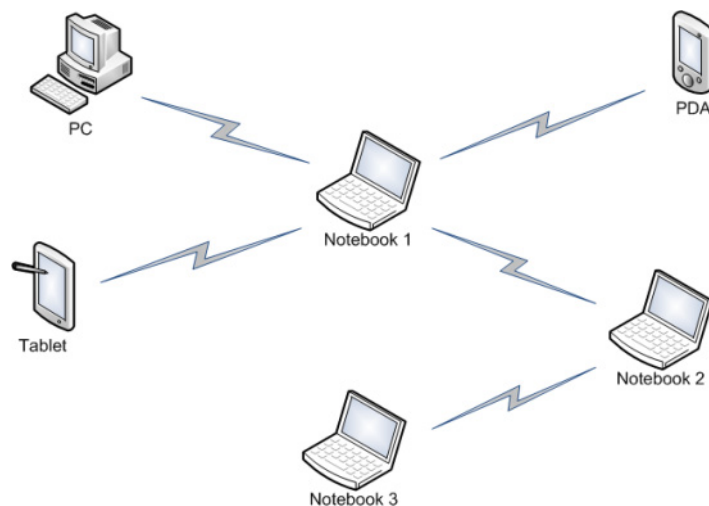
2.5 Topológia WLAN

Bezdrôtové zariadenia disponujú dvomi základnými možnosťami pripojenia. Ich použitie závisí od požiadavky na štruktúru siete. Prvým režimom je nezávislá sieť Ad-hoc, druhým zasa najčastejšie používaná sieť s presne vymedzenou infraštruktúrou.

2.5.1 Ad-hoc

Norma IEEE 802.11 špecifikuje tento režim, v ktorom nie je žiadny riadiaci prístupový bod (AP). Tá následne upravuje aj nutné požiadavky pre realizáciu siete. Je potrebné, aby všetky počítače v rámci ad-hoc režimu používali rovnaký kanál pásma 2.4 GHz a zároveň aj zhodné SSID¹⁰. Okrem zaužívaného označenia ad-hoc sa môžeme stretnúť s pomenovaním IBSS¹¹ alebo peer-to-peer (režim rovnocenných uzlov).

Najčastejším využitím je pripojenie niekoľkých klientov z určitého špecifického dôvodu na krátky čas. Presne takým motívom je hranie sieťových hier alebo presun súborov medzi klientmi. Ak je jeden z klientov konfigurovaný aby pracoval ako internetová brána, je prípustné aj zdieľanie prístupu do siete internet (Obrázok 2.9). Ich nízka obľúbenosť je spôsobená obmedzeným dosahom a pre bežného používateľa náročným procesom konfigurácie. Existuje mnoho médií, na ktorých je možné dáta prenášať efektívnejšie. (1)



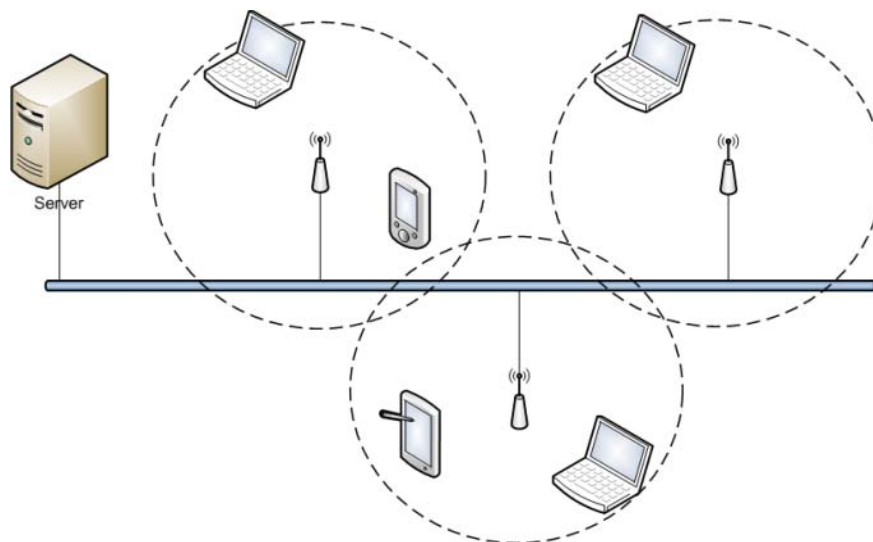
Obrázok 2.9 Grafické znázornenie ad-hoc

¹⁰ Skratka významu *Service Set Identifier*, čo znamená jedinečný identifikátor WLAN vysielaný AP.

¹¹ Skratka významu *Independent Basic Service Set*, čo predstavuje *Nezávislý základný súbor služieb*.

2.5.2 Infraštruktúra

V tejto sieti musí byť umiestnený minimálne jeden centrálny AP (Obrázok 2.10), ktorý je rozhraním medzi bezdrôtovou a drôtovou sieťou s funkciou dátového mostu. Klient sa po úspešnej asociácii k nemu pripojí, čím získa prístup do celej siete. Poskytuje väčšiu plochu pokrytia signálom pre značný počet klientov (zvyčajne max. 253). Rada výhod posúva do popredia práve infraštruktúru pred ad-hoc. Citlivou je otázka zahltenia pásma prenosom medzi klientmi, ku ktorému dochádza napríklad pri kopírovaní objemných dát. Aj tu sa núka riešenie vo verzii softvéru, ktorý je schopný obmedziť prenos na základe stanoveného limitu. (12)



Obrázok 2.10 Grafické znázornenie infraštruktúry

2.6 Hardware pre WLAN

Trh bezdrôtových sietí poskytuje široké spektrum zariadení, či už aktívnych alebo pasívnych. Aktuálne trendy implementujú Wi-Fi aj do výrobkov spotrebnej elektroniky ako HiFi súpravy, DVD prehrávače alebo TV.

WLAN periférie určené na výstavbu firemnej siete musia spĺňať vysoké kvalitatívne požiadavky na nepretržitú prevádzku, a to bez ohľadu na počiatočne náklady. Maskovaným nepriateľom kvality je ázijská produkcia neznačkových zariadení, ktorej stratégiou je nízka cena. Práve podradné prvky v bezdrôtovej sieti oslabujú jej celkovú štruktúru, lebo aj tu platí, že sieť je taká silná, ako jej najslabší článok. Na strane druhej, ak zvážime účel a možné riziká, ktoré nebudú výrazné, je použitie lacnejších periférií možné na domáce použitie.

Každá bezdrôtová jednotka sa skladá z čipovej sady a podpornej elektroniky s vysokofrekvenčným vysielačom a prijímačom. Má dve dôležité časti, ktoré dávajú priestor pre odlíšenie konkurencie. Predovšetkým to je *ovládaci softvér* pre správu zariadenia a *čipová sada*. (12)

2.6.1 Aktívne prvky

Bezdrôtový prístupový bod (AP) je zariadenie spájajúce bezdrôtové klienty, čím vytvára bezdrôtovú sieť. Jeho úlohou je poskytovať klientom prístup na internet a lokálnu sieť, udržiavať bezpečnosť siete a zaisťovať premostenie medzi LAN a WLAN.

AP môžeme rozdeliť do dvoch kategórií. Po prvé sú to zariadenia pre *potrebu stredných a veľkých podnikov*, majúce profesionálne funkcie sieťového manažmentu, podporu výkonných zabezpečovacích protokolov a integráciu s ostatnými zariadeniami v rozsiahlych sieťach. Ich dodávateľmi sú spoločnosti Cisco, Orinoco, Nokia a iné. Po druhé hovoríme o zariadeniach pre domáce použitie a malé firmy (pod skratkou SOHO¹²), ktoré poskytujú podobné funkcie ako profi verzie. Sú však kapacitne obmedzené a ich softvérové rozhranie je zamerané na bežného užívateľa so základnými znalosťami. Najviac sa pre jednoduchosť a možnosť aplikácie nápovedy využíva konfigurácia cez webové rozhranie.

¹² Skratka významu *Small Office/Home Office*, čo znamená pre *domáce použitie a malé firmy*.

Členením podľa funkcie poznáme router, opakovač a most. Router po zapojení k sieti internet spracuje vstupný signál a šíri ho ďalej bezdrôtovo a zvyčajne poskytuje aj funkciu prepínača pre LAN. Bezdrôtový opakovač zasa používame na rozšírenie dosahu existujúcej WLAN, pretože opakuje vysielaný signál hlavného AP. Most umožňuje preklenúť dve WLAN a vytvoriť tak kompaktnú širokú sieť. Niektorí výrobcovia poskytujú hybridné zariadenia, ktoré zvládajú obidve alebo dokonca všetky tri funkcie, pričom aktívna môže byť len jedna.

Klientske adaptéry, s ktorými dnes pracujeme sú už v prevažnej miere integrované na matičnej doske počítačov a notebookov. Okrem iných existujú externé zariadenia pre WLAN pripájané cez rozhranie USB 2.0, PCI a PCI expres, PCMCIA pre notebooky. Pre zlepšenie dosahu zariadenia sa namiesto integrovaných antén zavádzajú externé antény s vyššou ziskovosťou. (1)

2.6.2 Antény

Žiadna WLAN sa nezaobíde bez kvalitnej antény. Antény dodávané s jednotlivými zariadeniami sú postačujúce pre pokrytie interiéru a pre exteriér sa používajú násobne výkonnejšie antény s určitým uhlom vyžarovania určeným podľa lokálnych podmienok a potrieb.

Základné je rozdelenie antén podľa markantných vlastností:

Smerovosť antén znamená smer, do ktorého je distribuovaný signál. Podľa toho sa ďalej diverzifikujú na všesmerové, sektorové a smerové (Obrázok 2.10).

Všesmerové antény šíria signál do všetkých strán vykrývajúc uhol 360 stupňov a ich aplikácia je na miestach potreby súvislého pokrytia. Prevažná časť AP je dodávaná práve s týmito anténami.

Sektorové antény vyžarujú do určitého uhla. Uplatnenie nachádzajú v oblastiach, kde je potrebné vykryť špecificky vymedzené oblasti a tým aj zabrániť šíreniu signálu mimo stanovenú oblasť.

Smerové antény sú podskupinou sektorových antén. Ide o smerové parabolické antény typu sito alebo Yagi najčastejšie používané na dlhé vzdialenosti. Lúč je úzko smerový, vyžarovaný do jedného bodu.

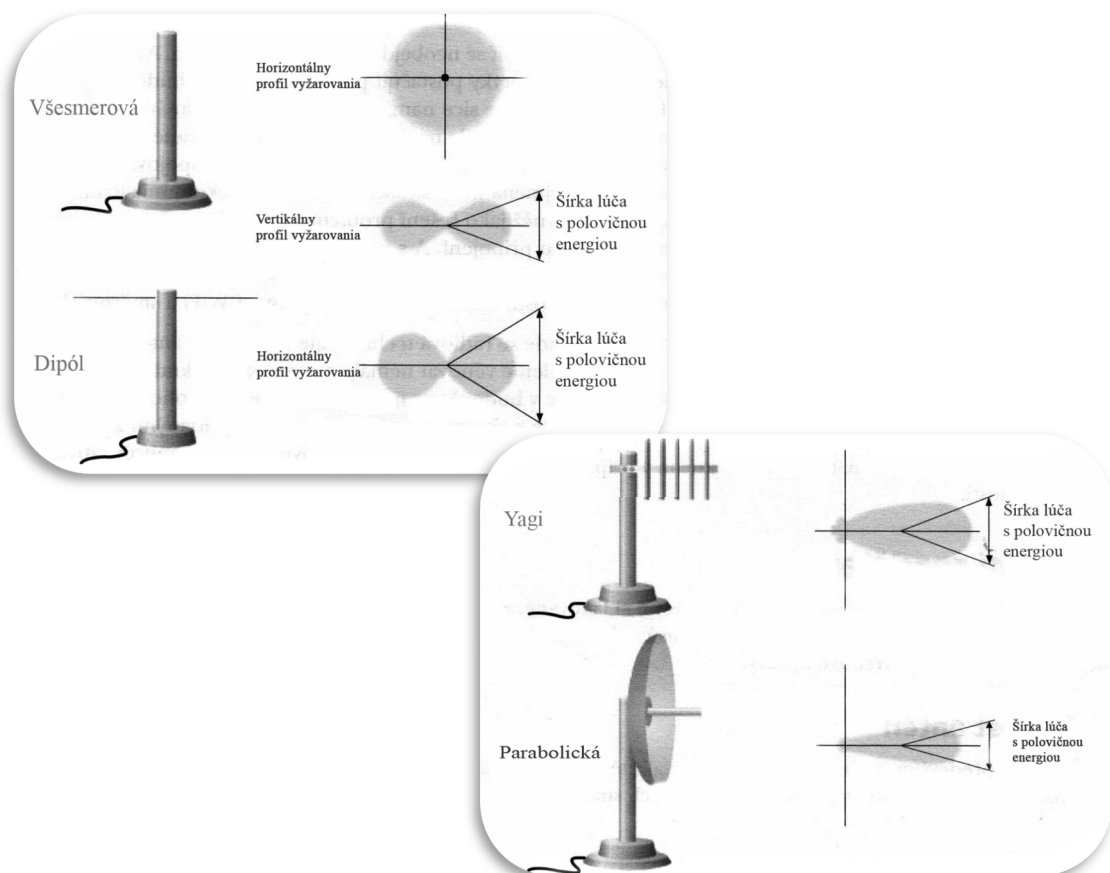
Zisk antén je pomer medzi intenzitou vyžarovania v danom smere k intenzite vyžarovania, ktorú by sme dostali, ak by energia prijatá anténou bola vyžiarená

rovnomerne do všetkých smerov. Zisk sa udáva v jednotkách decibelov na izotrop (dBi).

Polarizácia elektromagnetického vlnenia má dva typy a to *lineárnu a kruhovú*. *Lineárna polarizácia* sa v praxi používa horizontálna a vertikálna. *Kruhová polarizácia* môže byť pravotočivá alebo ľavotočivá. Rovina polarizácie závisí plne na konštrukčnom riešení antény.

Vyžarovací uhol definuje, do akého smeru a pod akým uhlom anténa vyžaruje. Existuje horizontálny a vertikálny. Horizontálny uhol vyžarovania je v prípade všesmerových antén 360 stupňov. Vertikálny vyžarovací uhol vymedzuje výšku vyžarovacieho kužeľa.

Vzhľad antény. Dôležitým parametrom každej vonkajšej antény sú jej rozmery a váha, čo nám určuje možnosti uchytenia. Parabolické antény sú náchylné na náporu vetra. Sektorové a všesmerové antény sú umiestnené do malých plastových valcov, na ktoré je vplyv počasia minimálny. Vnútorne antény nevyžadujú ochranu proti poveternostným vplyvom, ale sú zamerané na dizajn a vkusné prevedenie. (12)



Obrázok 2.11 Základné typy antén (12)

2.7 Ochranné prvky a metódy útokov na WLAN

Bezdrôtová sieť má v porovnaní s káblovou jednu eminentnú nevýhodu vyplývajúcu z jej princípu - nie je možné dostatočne obmedziť priestor dostupnosti siete. Pomocou ľahko prístupných softvérových nástrojov ako napríklad NetStumbler, AirSnort, AiroPeek a množstva návodov k ich použitiu, dokáže aj menej skúsený používateľ prekonať slabšie zabezpečený AP (WEP, MAC filter) a preniknúť tak k zraniteľným dátam. Prevláda povedomie, že ak sa v sieti neoperuje s citlivými dátami, ako napríklad v domácej sieti, nie je potrebné sa zaťažovať zabezpečením WLAN. Musíme si však uvedomiť, že pri každej WLAN sieti je aj pripojenie do internetu, čo je platená služba s prevažne obmedzenou šírkou pásma. Ak útočník vstúpi do nechránenej siete, dokáže v nej vytvoriť veľký tok dát a tým čiastočne obmedziť alebo úplne zahltiť celé poskytnuté pásmo.

Kvalitné zabezpečenie bezdrôtovej siete, najmä firemnej, rozhodne nepatrí medzi triviálne záležitosti a svojou zložitosťou ochrany na niekoľkých vrstvách vyžaduje neustálu kontrolu a aktuálnosť spravovanú odborníkom na danú oblasť.

V mnohých prípadoch sa pri vytvorení silnej bezpečnostnej bariéry pozabúda na maličkosti, ktoré značne uľahčia prístup do siete, a tým eliminujú všetky profesionálne zabezpečovacie systémy.

2.7.1 Primárne zabezpečenie

Prvým a nie menej dôležitým krokom zabezpečenia WLAN je *zmena výrobných nastavení hesiel zariadení*, ktoré nimi disponujú. Z logického hľadiska ide o významné opatrenie, ktoré pri nedodržaní spôsobí plné otvorenie systému bezdrôtovej siete na jej správu. Strategickým rozhodnutím je implementácia možnosti *zákazu správy zariadenia inou cestou ako metalickou sieťou*. Pre lepšie priblíženie si predstavme hardvérový firewall s povolenou správou cez WLAN pomocou web rozhrania.

Výkonné a kvalitné zariadenia typu AP alebo firewall prípadne spravovateľný prepínač sa konfiguruje cez Telnet. Pozitíva správy použitím web rozhrania sa však stále viac rozširujú a získavajú si širokú odbornú verejnosť.

2.7.2 Hide SSID

Jednou z najjednoduchších ciest ochrany bezdrôtovej siete je skrytie alebo zastavenie vysielania identifikátora siete SSID. Ešte predtým by sa mala vykonať zmena prednastaveného názvu SSID na vlastný názov, čo síce nijaké zvýšenie bezpečnosti neprinesie, ale útočníkovi to naznačí, že v zariadení bola zmenená konfigurácia výrobcu. Pre oprávnených klientov v sieti nie je funkcia skrytia identifikátora obmedzujúca. Postačuje nastaviť v operačnom systéme profil bezdrôtovej siete so správnym názvom SSID.

Skrytie SSID môže i napriek tomu, že ide pre útočníka o ľahko odstrániteľný prvok zabezpečenia, zmeniť jeho voľbu pri výbere zraniteľnej siete.

Existuje niekoľko programov, schopných okrem iného, v priebehu pár sekúnd detegovať vysielaný identifikátor siete. (5)

2.7.3 Filtrovanie adries

Každé sieťové rozhranie je vybavené unikátnou fyzickou adresou MAC, ktorá má dĺžku 48 bitov. Práve na základe tohto identifikátora je u väčšiny AP alebo firewall nastaviteľný zoznam MAC adries povolených pre prístup k sieti. Neskôr sa objavil aj tzv. Blacklist, čo je variant zoznamu MAC adries, ktoré majú blokovaný prístup .

Z pohľadu užívateľa je MAC adresa nemenná. Nie je tomu tak, ide o programovateľnú informáciu ukladanú do firmvéru zariadenia, ktorú je možné zmeniť. To znamená možnosť obísť filtrovanie podľa MAC adries. Toto pasívne zabezpečenie sa odporúča zavádzať v malých firmách a domácnostiach, lebo trvalé udržiavanie aktuálneho zoznamu platných MAC adries je nereálne pri väčších počtoch klientov.

Metóda prelomenia opatrenia sa nazýva MAC spoofing, čo je technika zmeny MAC adresy zariadenia útočníka na adresu v zozname povolených MAC v AP. Proces je plne automatizovaný dostupným softvérom a zvyčajne netrvá dlhšie než pár sekúnd. Iným variantom je útok deautentizácie, ktorého zámerom je prinútiť klienta znova k autentizácii, kde sa následne využije metóda MAC spoofing. (12)

2.7.4 WEP

Štandard pre zabezpečenie rádiovkej časti siete ako súčasť IEEE 802.11 od roku 1999. Jeho cieľom bolo zabezpečiť ochranu rovnocennú drôtovým sieťam. WEP používa symetrickú streamovú šifru RC4 (šifru s tajným kľúčom) pre utajenie informácií a pre verifikáciu ich zhody metódu CRC-32 kontrolného súčtu. Podstatou tejto šifry je, že sa odosielaná správa zašifruje podľa určitého kľúča a na cieľovom bode sa opätovne pomocou zvoleného kľúča dešifruje. Kľúč je však ešte doplnený inicializačným vektorom IV o dĺžke 24 bitov. Najprimitívnejší variant je 64 bitový WEP kľúč, nasleduje 128, 256 a 512 bitová verzia. Bezpečnosť RC4 závisí práve na dĺžke kľúča a na počte jeho obmien. Tu narážame na problém distribúcie kľúča, ktorú WEP nerieši a pri nesprávnom doručení existuje riziko odhalenia.

V roku 2000 sa objavili prvé oficiálne dokumenty, ktoré poukazovali na slabinu algoritmu šifry RC4. Tá tkvie predovšetkým v približnej známosti vzhľadom na inicializačný vektor IV, čiže v možnosti rozlúštiť kľúč. Predlžovanie kľúča má k dĺžke jeho lámania lineárnu závislosť, takže predĺženie kľúča na jeho štvornásobok predĺži aj čas na jeho lámanie ale iba štvornásobne. (13)

Známy program k rekonštrukcii WEP kľúčov pod názvom AirSnort pracujúci pod operačným systémom Linux uviedli v roku 2001 ako voľne šíriteľný. Jednoduchým ovládaním umožňuje používanie aj málo pokročilým používateľom. K rozlúšteniu potrebuje 5 až 10 miliónov paketov. Uvoľnenie programu prinieslo so sebou významný efekt, ktorý plne vplýval na urýchlenie vývoja bezpečnejšieho štandardu zabezpečenia 802.11 sietí. (12)

2.7.5 WPA

Ako záplata pre nepostačujúci štandard zabezpečenia WEP bol vydaný v roku 2003 nový bezpečnostný mechanizmus ratifikovaný Wi-Fi alianciou. Jeho jadrom bol mechanizmus zo vznikajúceho štandardu 802.11i použitý pre šifrovanie komunikácie a riadenia prístupu do siete.

TKIP (Temporal Key Integrity Protocol), používaný pre šifrovanie komunikácie, uplatňuje rovnaký šifrovací algoritmus ako WEP, s rozdielom využitia 128 bitového kľúča a jeho dynamickou zmenou. Ďalšie novum prišlo s použitím kontroly integrity

správ (Message Integrity Check – MIC), ktorá má za cieľ znemožniť útočníkovi zmenu správy po prenose. (12)

Výhodou WPA je podpora dynamických kľúčov využívaných v podnikových sieťach. Distribúcia kľúčov tu využíva štandard 802.1X na protokole EAP (Obrázok 2.12). Nevyhnutné je použitie infraštruktúry so serverom RADIUS. Pre domáce siete sú určené nastaviteľné zdieľané kľúče PSK¹³ známe aj ako personálne kľúče.

Dvojica bezpečnostných expertov z Nemecka našla v roku 2008 variantu praktického útoku voči zabezpečeniu WPA. Vo svojej postate sa jedná o útok vloženým paketom. Následne v roku 2009 japonský kryptológovia zlepšili tento útok na WPA, ktorý je možné použiť aj v scenároch, kde pôvodný útok zlyhal. (14)

2.7.6 WPA2

V júni roku 2004 bol definitívne schválený štandard IEEE 802.11i, ktorý dostal komerčný názov WPA2. Zásadným rozdielom oproti WPA je použitá bloková šifra AES, ktorú kompletizovala a testovala približne päť rokov americká vláda. Je ponechaná aj možnosť návratu k TKIP šifre kvôli zlučiteľnosti s WPA. Pre plné užívanie možností WPA2 je potrebné nové zariadenie schopné efektívne využívať plnú silu AES šifry.

AES (CCMP¹⁴) využíva symetrický kľúč pre šifrovanie a dešifrovanie. Dĺžka kľúča sa pohybuje v rozmedzí 128 až 256 bitov. AES šifruje dáta postupne v blokoch (odtiaľ názov bloková šifra) o dĺžkach 128 bitov. Prednosťou je vysoká rýchlosť náročného šifrovania a doposiaľ nenájdená metóda prelomenia šifry.

WPA2, ako aj WPA, je predurčený pre podnikové prostredie, kde vystupuje pod názvom WPA2 Enterprise. Autentizačná metóda 802.1X/EAP aplikujúca predvolenú šifru AES, využíva RADIUS server. Domáce prostredie pokrýva metóda PSK, zdieľaného kľúča, ktorý pozostáva z frázy 8 až 63 znakov, ktorá je ďalej šifrovaná pomocou TKIP alebo AES. (15)

¹³ Skratka významu *Pre-Shared Key*, čo znamená *pred zdieľaný kľúč*.

¹⁴ Skratka významu Counter Mode Cipher Block Chaining- Message Authentication Code Protocol, v podstate algoritmus obsahujúci AES šifru.

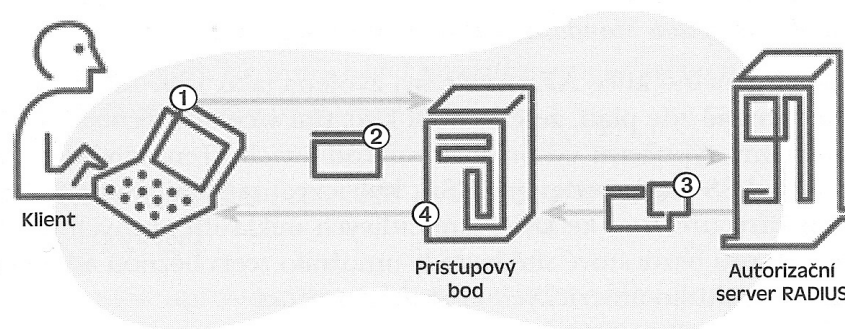
2.7.7 Autentizácia 802.1X

IEEE 802.1X je všeobecný bezpečnostný rámec pre všetky typy sietí zahrňujúci autentizáciu užívateľov, integritu správ a distribúciu kľúčov. 802.1X blokuje prístup k segmentu lokálnej siete pre užívateľov bez adekvátneho oprávnenia. Je vystavaný na protokole EAP¹⁵ a prenáša pakety cez spojovú vrstvu LAN. Správy EAP sa zapuzdrujú do rámcov 802.1X.

Overovanie v bezdrôtovej sieti zaisťuje AP pre klientov na základe ich výzvy, pomocou zoznamu alebo externého autentizačného serveru RADIUS. Iba overený používateľ má možnosť prístupu k WLAN.

Obrázok 2.12 znázorňuje kroky autentizácie podľa 802.1X:

- 1) Klient odošle počiatočnú správu na AP, ktorý odpovie požiadavkou na identitu klienta správou EAP REQUEST-ID.
- 2) Klient odpovie správou EAP RESPONSE-ID, ktorá obsahuje identifikačné údaje používateľa. AP zapuzdří celú správu do paketu RADIUS ACCESS_REQUEST a pošle ju autorizačnému serveru RADIUS.
- 3) Server RADIUS odpovie správou obsahujúcou povolenie/zákaz prístupu pre daného klienta do siete (RADIUS ACCESS_ACCEPT/DENY), ktorá v sebe obsahuje informáciu EAP SUCCESS/FAILURE, ktorú AP prepošle klientovi.
- 4) V prípade povolenia (SUCCESS) je príslušný port prístupu do siete otvorený pre dáta autentizovaného používateľa. (12)



Obrázok 2.12 Autentizácia podľa 802.1X (12)

¹⁵ Skratka významu Extensible Authentication Protocol, znamená rámec poskytujúci prenos a používanie zakľúčovaného materiálu.

3 ANALÝZA PROBLÉMU A SÚČASNÁ SITUÁCIA

Moderné spoločnosti čoraz viac inklinujú k využívaniu pružnosti ich zamestnancov, preto ich prestávajú viazať na statické PC a kancelárie dopĺňajú o prenosné počítače s integrovaným bezdrôtovým rozhraním podporujúcim štandardy 802.11b/g/n. To so sebou prináša výhodu mobility a možnosti práce prakticky na akomkoľvek mieste. Výsledným efektom je zvýšená produktivita zamestnancov prinášajúca spoločnosti lepšie výsledky a skrátenie doby potrebnej na úspešné zvládnutie zadanej úlohy. Ruší sa aj problém presunu metalických vodičov v prípade premiestnenia vybavenia kancelárie.

Vytvorenie kvalitnej firemnej bezdrôtovej siete požaduje profesionálny prístup, plánovanie už pri výstavbe/rekonštrukcii objektu a nemalú časovú a finančnú náročnosť. Východiskový plán umiestnenia AP z dôvodu pokrytia bezdrôtovým signálom celého objektu býva mnohokrát nepresný, prípadne ak sa vyskytnú nepredvídané okolnosti a prekážky, aj nepoužiteľný. V konečnom dôsledku sa každá chyba a nepresnosť odráža vo finálnej výške nákladov. Pre firemné prostredie, kde sa jedná o veľké plochy, môže dôjsť k zrušeniu projektu z dôvodu výrazného prekročenia rozpočtu.

Ak fáza plánovania prebehne v poriadku a umiestnené AP pokrývajú všetky požadované miesta bez veľkého presahu, prichádza rada iných problémov. Logickým problémom je prechod medzi jednotlivými AP (tzv. roaming), kedy dochádza k anulovaniu asociácie s AP a tým aj prerušeniu dátového toku a potrebe reasociácie. Ďalším, už podrobnejšie spomínaným problémom, je hustota kanálov v pásme ISM a ich vzájomné interferencie, ktoré prakticky neumožňujú koexistenciu viacerých sietí s blízkymi kanálmi.

Všetky tieto a aj veľa iných prekážok zdoláva systém bezdrôtových sietí štvrtej generácie.

3.1 Firemná WLAN v ohrození

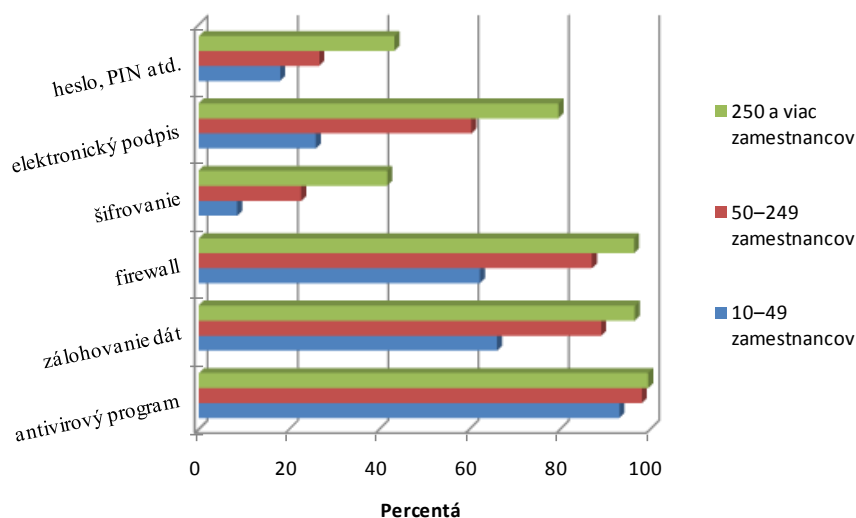
Z prieskumu spoločnosti Vanson Bourne organizovaného na vzorke 400 vedúcich pracovníkov IT vyplynulo, že v roku 2009 svoje dáta vo WLAN kódovalo menej než 50 % firiem v Európe.

Výsledky ďalej uvádzajú, že viac ako 64 % organizácií zanedbáva bezpečnosť svojich WLAN a viac než polovica spoločností aplikuje zhodné opatrenia pre LAN a WLAN. Sám hlavný technolog spoločnosti *Motorola Enterprise Wireless LAN* uviedol ako prekvapujúci fakt, že firmy nevyužívajú robustné štandardy pre kódovanie WPA2, ale stále sa pridávajú nekvalitného a ľahko prelomiteľného bezpečnostného štandardu WEP.

Alarmujúci je aj údaj, ktorým z 56 % firiem pripúšťa silné obavy z narušenia bezpečnosti dát a to u zamestnancov mimo kanceláriu, kde sú citlivé dáta posielané cez nezabezpečené siete internetových kaviarní bez použitia bezpečného tunela VPN.

Neefektívnosť využívania pracovného času vnímajú mnohí správcovia IT. Len málokto z nich je však ochotný zmeniť svoje stereotypy. Až 58 % z nich trávi viac ako dve hodiny týždenne hľadaním neautorizovaných AP, pričom existuje riziko zabudnutia na iné, závažnejšie hrozby. I keď je táto činnosť potrebná, lepšie výsledky je možné dosiahnuť jej automatizáciou. (16)

Stav slabého zabezpečenia firemnej siete ako celku (nie len WLAN) najmä u malých firiem potvrdzuje graf štatistického úradu (Obrázok 3.1). Iba 10 % podnikov využíva šifrovanie. (17)



Obrázok 3.1 Graf zabezpečenia ICT v podnikoch (2009) (17)

3.2 Aktuálny stav

V súčasnosti spoločnosť plánuje vybudovanie WLAN siete v modernej budove ich sídla a zároveň aj prevádzky hotela (Obrázok 3.2). Požadovaná konfigurácia má nastavenú hladinu bezpečnosti časti pre zamestnancov pomocou štandardu 802.11i (WPA2) a autentizácia prebieha cez bezpečnostný rámec 802.1X na RADIUS server.

WLAN určená klientom hotela bola spustená v januári 2009 a pozostáva z AP pripojeného do lokálnej siete s prístupom na internet oddelenej firewallom.

Spoločnosť kladie požiadavku na vytvorenie kompaktnej siete bez obmedzení spôsobené roamingom medzi AP, vzhľadom na to že využíva VOIP¹⁶. Intenzita signálu musí byť dostatočná na celom hlavnom poschodí, kde sú kancelárie, a strediská recepcia, bar, reštaurácia a letná záhrada s terasami (rozmiestnenie podľa pôdorysu).

Využíva optické pripojenie do siete internet, čo zabezpečí dostatočnú prenosovú rýchlosť pre všetkých užívateľov.



Obrázok 3.2 Hotel International **** (18)

¹⁶ Skratka významu *Voice Over Internet Protocol*, čo znamená *prenos hlasu pomocou internetového protokolu*.

4 VLASTNÝ NÁVRH RIEŠENIA

Vzhľadom k úzkej spolupráci so spoločnosťou a akútnej potrebe riešenia ich problému s modernizáciou pracovného procesu je vypracovaný tento návrh bezdrôtovej siete WLAN v objekte firmy.

4.1 Predstavenie spoločnosti

Golf International spol. s r. o. poskytuje hlavne služby v oblasti golfu. Prevádzkuje golfový rezort Black Stork s 27 jamkami taktiež hotel International ***** s celoročnou prevádzkou lokalizovaný v obci Veľká Lomnica.

Sortiment poskytovaných služieb na golfovom ihrisku Black Stork:

- ◇ 18 + 9 jamkové ihrisko (International, Panorama, Village)
- ◇ Putting & Chipping range (cvičný putting a chipping)
- ◇ Driving range (cvičné odpalisko)
- ◇ Golfová recepcia a Golf shop
- ◇ Požičovňa príslušenstva
- ◇ Golfový simulátor

*Sortiment poskytovaných služieb v hoteli International*****:*

- ◇ Ubytovanie v 28 2-lôžkových izbách + 1 apartmán
- ◇ Reštaurácia, Lobby bar
- ◇ Vonkajší (vyhrievaný) a vnútorný bazén
- ◇ Konferenčná miestnosť
- ◇ 24h recepcia
- ◇ Bezplatné pripojenie k internetu (na izbách i verejných priestranstvách)
- ◇ Sauna (parná, infra, suchá)
- ◇ Indoorbar

4.2 Pôdorys hlavného podlažia hotela

Legenda:

1 Recepčia

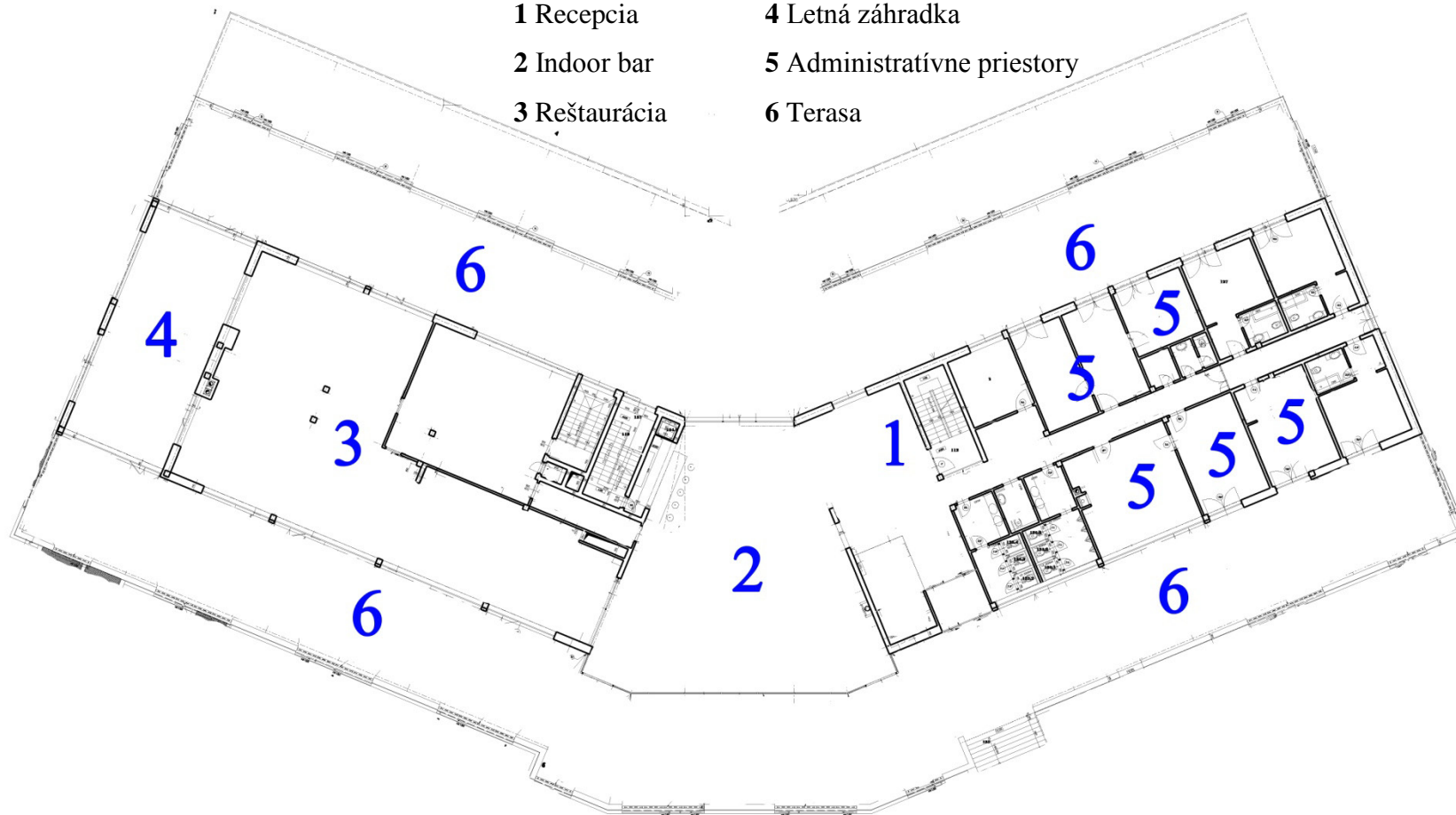
2 Indoor bar

3 Reštaurácia

4 Letná záhradka

5 Administratívne priestory

6 Terasa



4.3 Priblíženie podstaty riešenia

Viacrát spomínaná technológia štvrtej generácie je tým pravým riešením, ktoré smeruje do budúcnosti a eliminuje možnosť zastarania systému po dobu minimálne štyroch rokov.

Charakteristika systému zmienená v kapitole 2.4.7 akcentuje na prioritách ako garancia priepustnosti, pokrytia a mobility.

Izraelská spoločnosť EXTRICOM, ako dizajnér a výrobca bezdrôtového systému reprezentujúceho novú generáciu infraštruktúry WLAN, vyvinula tento unikátny systém jednoduchý na spravovanie. Podpora štandardov 802.11a/b/g/n, patentovaná technológia Interference-Free (bez interferencií) a centralizovaná správa všetkých ultratenkých AP ešte viac zvyrazňujú jej výhody.

Na rozdiel od existujúcich tzv. bunkových sietí, kde každé AP sa správa autonómne, je blanket technológia charakteristická práve pokrytím veľkých priestorov umiestnením viacerých ultra tenkých AP. Ultra tenké AP znamená zariadenie prístupového bodu s minimalizovanou, alebo žiadnou inteligenciou, pričom tá je koncentrovaná do centrálného riadiaceho prvku typu prepínač. Klesajú tým výrobné náklady na AP, zaniká variant napadnutia softvéru a nežiaduca zmena jeho konfigurácie. Ovládacím prvkom je skutočne jedinečný prepínač so špeciálnym firmvérom pre správu.

4.4 Výber vhodného hardvéru

4.4.1 EXSW – 1200

Nová generácia prináša aj nové zariadenia. Centrálnym riadiacim prvkom všetkých ultratenkých AP bude prepínač (switch) EXSW – 1200 (Obrázok 4.1) kompatibilný so štandardmi IEEE 802.11a/b/g. Zariadenie má 12 ethernetových 10/100 Mbps portov a dva extra 100/1000 Mbps porty pre pripojenie k hlavnému switchu siete tzv. uplink. Dokáže kontrolovať až štyri blankety (vrstvy) WLAN súčasne, bez ohľadu na zvolené pásmo.

Pre každý kanál, sa dá limitovať pridelená šírka pásma nasledovne:

- 802.11b – 1 až 11 Mbps
- 802.11g – 1 až 54 Mbps
- 802.11a – 6 až 54 Mbps

Bezpečnosť dát je chránená šifrovaním WEP-64, WEP-128, WPA-TKIP/AES alebo WPA2-TKIP/AES. Autentizácia do siete prebieha pomocou RADIUS servera (802.1X) a autentizačného rámca EAP metódami TLS, LEAP, PEAP alebo MD5. Pre zobrazenie úvodnej uvítacej stránky a oddelenie siete je použiteľná Captive portal autentifikácia aplikovateľná v našom prípade pre pripojenie hostí/klientov. Primárny prístup na stránku spoločnosti umožňuje Captive portal walled garden.

Výhodou je funkcia priradenia každej sieti (vrstve) samostatný súbor bezpečnostných pravidiel. Zabudovaná automatická detekcia narušenia bezdrôtovej siete zaznamenáva a hlási tieto stavy správcovi siete. Skenovanie podvrhnutých AP prebieha v rámci softvéru prepínača a za pomoci AP automaticky.

Všetkých dvanásť ethernetových portov podporuje technológiu POE, čím dodáva elektrickú energiu a dáta ultratenkým prístupovým bodom, všetko v jednom sieťovom kábli osadenom štyrmi párami krútených dvojliniek.

Správa zariadenia je realizovaná cez zabezpečené grafické užívateľské rozhranie pracujúce v okne internetového prehliadača alebo klasicky formou príkazového riadku. Rovnako je aktuálny firmvér nahrávaný prostredníctvom spomínaných rozhraní GUI¹⁷ alebo CLI¹⁸.



Obrázok 4.1 Dvanásť portový switch pre AP (19)

¹⁷ Skratka významu *Graphic User Interface*, v preklade grafické užívateľské rozhranie.

¹⁸ Skratka významu *Command Line Interface*, v preklade rozhranie príkazového riadku.

4.4.2 EXRP – 40

Prístupový bod EXRP – 40 (Obrázok 4.2) je ultratenký, preto neobsahuje žiadny konfiguračný softvér. Jeho úlohou je pracovať ako predĺžená ruka centrálného prepínača. Má integrované štyri rádiové moduly s dvojitémi anténami, kde každý môže vysielat' na jednom z troch neprekrývajúcich sa kanálov. Podporuje štandardy IEEE 802.11a/b/g.

Spomínaná funkcia vyhľadávania podvrhnutých AP kontroluje priestor v priemere každé 2 minúty.

Napájanie je vyriešené systémom POE.



Obrázok 4.2 Štvorrádiový AP 802.11a/b/g (20)

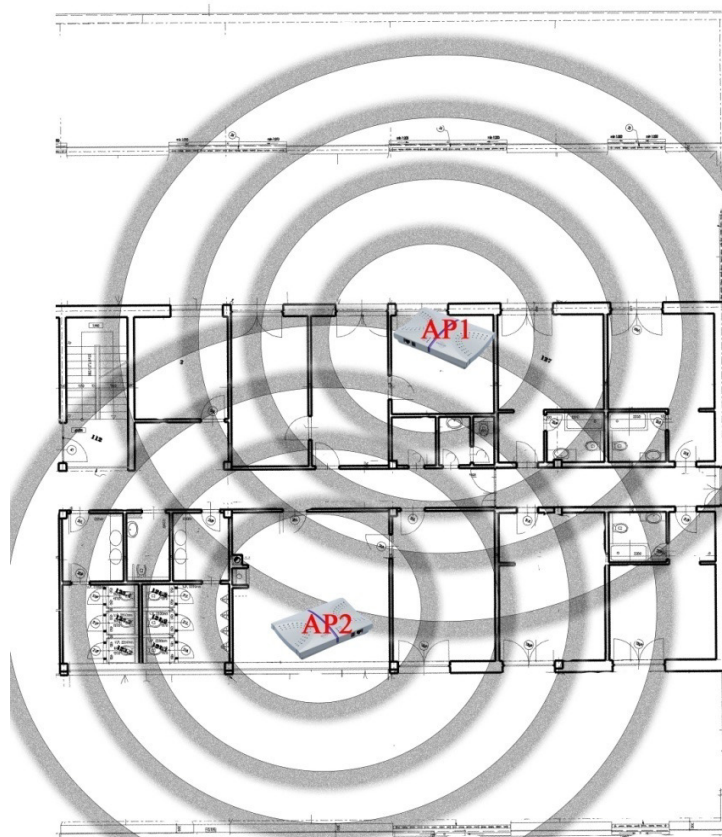
4.5 Rozmiestnenie hardvéru

V kapitole 2.4.7 je zmienené heslo *čím viac AP, tým lepšie pokrytie*. U Wi-Fi štvrtej generácie skutočne nie je potreba zložitého komplexného RF (Radio Frequency) prieskumu a používanie sofistikovaného softvéru pre výpočet interferencií a strát signálu v priestore. Úplne postačuje aj hodinová prehliadka priestorov, kde bude technológia použitá a následne zaznamenanie vhodného bodu umiestnenia AP (z estetickej a funkčnej stránky).

Centrálne riadiaca jednotka je umiestnená do racku v serverovni, odkiaľ vedú ethernetové káble k jednotlivým AP.

4.5.1 Poloha AP v administratívnej zóne

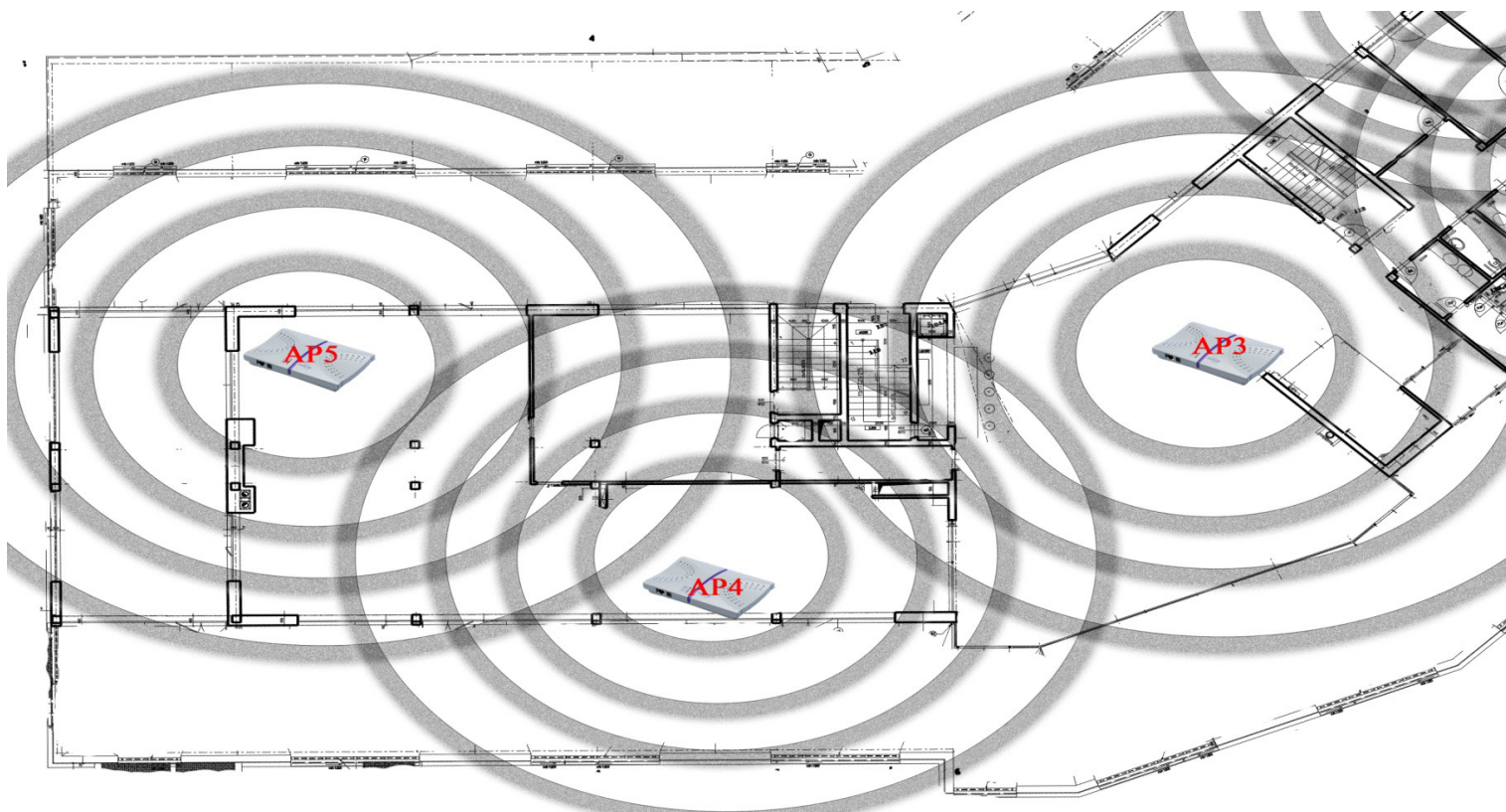
Prístupové body umiestnené v oblasti kancelárií plne pokrývajú všetky kancelárie a priestor terás v ich okolí. Znázornené šírenie elektromagnetických vln má odhadový charakter a nie je podložené RF meraním (čo ako už bolo spomenuté nie je potrebné). Rozmery priestoru pokrytia sú 25 x 31 metrov, preto je postačujúci počet AP dva.



Obrázok 4.3 Umiestnenie AP v administratívnej zóne

4.5.2 Poloha AP v hotelovej zóne

Hotelová zóna zahŕňa recepciu, Lobby bar, reštauráciu, letnú záhradu a terasy. Objekt, s plochou 1300 m² má v tejto časti prevažne obvodové vitríny namiesto klasickej pevnej steny. To prispieva k lepšiemu šíreniu signálu a nutnosti inštalácie len troch prístupových bodov pokrytia. Rozmiestnenie zabezpečí v okrajových bodoch objektu intenzitu signálu bezdrôtovej siete približne 54 %.



Obrázok 4.4 Umiestnenie AP v hotelovej časti

4.6 Konfigurácia siete a zariadení

4.6.1 Blanket Zamestnanci_International

Nastavenie bezdrôtovej siete musí spĺňať nároky spoločnosti. Prioritou je konfigurácia vrstvy (blanketu) pre zamestnancov v administratívnej časti. S použitou vyspelou technológiou budú môcť pracovať nielen vo svojich kanceláriách, ale na celom hlavnom poschodí a príľahlých terasách. V prípade potreby expanzie pokrytia signálom v exteriéri sa môžu využiť AP s konektormi pre pripojenie externých antén.

Pri paralelnej existencii viacerých bezdrôtových sietí môže dôjsť k situácii, kedy klienti nebudú vedieť, ktorá sieť je určená práve pre nich. Tomu zabraňuje vypnutie vysielania SSID blanketu pre zamestnancov.

V centrálnom prvku nastavíme:

- štandard 802.11g,
- limit pásma bez limitu,
- SSID Zamestnanci_International,
- kanál 11 (2,463 GHz),
- zabezpečenie WPA2,
- autentizácia 802.1X (RADIUS),
- ostatné nevysiela SSID.

4.6.2 Blanket Hot-Spot_International

WLAN primárne pre klientov hotela lokalizovaná v spoločných priestoroch recepcie, baru reštaurácie a teras má viacero reálnych riešení. Ťažiskom oboch systémov je zachovanie voľného prístupu do siete internet, separácia od firemnej siete a použitie Captive portal. Prvým je prístup na internet po zadaní hesla, ktoré si klient vyzdvihne na recepcii hotela. Druhým spôsobom nie je nutné zadávať žiadne prihlasovacie údaje, iba súhlasiť s podmienkami používania.

Vedenie spoločnosti Golf International s. r. o. zvažilo všetky realizovateľné varianty a rozhodlo sa implementovať nastavenie klientskej bezdrôtovej siete bez prihlasovacích údajov.

Pri konfigurovaní prepínača EXSW – 1200 aktivujeme funkciu Captive portal. Ďalším krokom je nastavenie stupňa autentifikácie na užívateľskú úroveň. Na lokálnom

serveri uložíme vytvorenú web stránku prihlásenia obsahujúcu informáciu o možnom bezpečnostnom riziku vstupu na internet a podmienky pripojenia. V rozhraní nastavenia uložíme odkaz na umiestnenie úvodnej web stránky. Pole odkazu na presmerovanie vyplníme linkom domovskej stránky spoločnosti, čím sa dosiahne, že po odsúhlasení podmienok užívania klientom sa zobrazí nie jeho stránka predvolená v prehliadači, ale web spoločnosti Golf International spol. s r.o. s adresou www.golftatry.sk. Posledný krok, izolácia od firemnej siete, sa zaistí prostredníctvom virtuálnej lokálnej siete VLAN mapovanej na SSID Hot-spot_International a odobratím práv k prístupu.

Nastavenie centrálného prvku pre sieť klientov:

- štandard 802.11g,
- limit pásma max. 24 Mbps,
- SSID Hot-spot_International,
- kanál 6 (2,437 GHz),
- zabezpečenie žiadne,
- ostatné používa Captive portal.

4.6.3 Blanket Administrácia

Vrstva pre celkovú správu firemnej siete je aktivovaná len na AP1 (kancelária správcu siete). Prístup k nej má povolený len administrátorovi. Má najväčšie práva v celej sieti. Používa rovnaký proces autentizácie ako zamestnanci tzn. 802.1X pomocou RADIUS servera.

Nastavenie prepínača pre AP1:

- štandard 802.11a,
- limit pásma bez limitu 54 Mbps,
- SSID Admin_International,
- kanál 5,30 GHz,
- zabezpečenie WPA2,
- autentizácia 802.1X (RADIUS),
- ostatné nevysiela SSID.

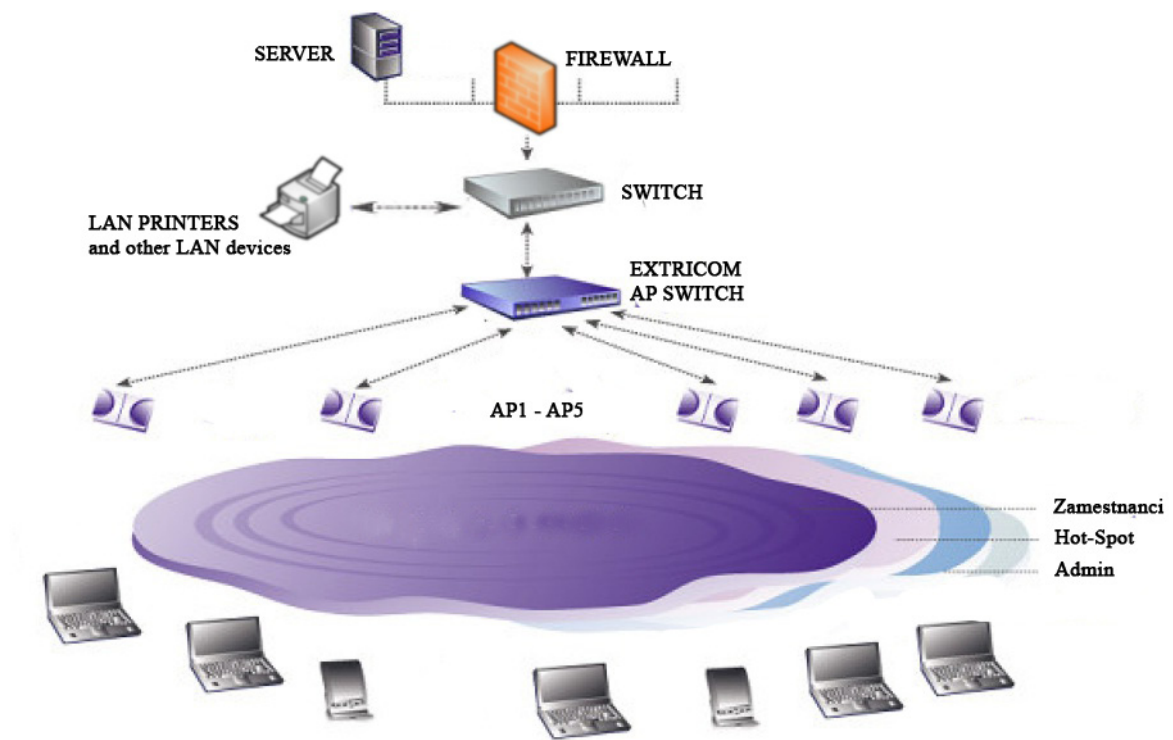
V prílohe sú pre vizuálne priblíženie zobrazené snímky obrazovky s najdôležitejšími nastaveniami prepínača EXSW – 1200.

4.6.4 Ostatné periférie

Zakúpené notebooky pre zamestnancov majú integrovaný čip rádiového rozhrania štandardu IEEE 802.11b/g/n s plnou podporou WPA/WPA2. Operačný systém Windows 7 disponuje funkciou vytvorenia profilu bezdrôtovej siete. Vzhľadom k skrytému identifikátoru siete zamestnancov predstavuje vhodný variant riešenia pre korporátne prostredie, kde je potreba distribuovať zhodné nastavenia na viaceré počítače.

Integrácia vstupno – výstupných zariadení (tlačiarne, skenery, fax) do LAN ostáva zachovaná, pomocou liniek ethernetového káblu.

Všetky dáta vstupujúce i vystupujúce z podnikovej siete z vonkajšieho prostredia sú filtrované cez hardvérový firewall ZyWALL USG 2000 obsahujúci aj antispam, antivírusový softvér. Účinne dokáže blokovať torrenty, peer-to-peer sťahovanie a v prípade výpadku optického pripojenia aktivuje záložný systém na báze 3G siete a automaticky obmedzí tok dát pre menej dôležité procesy.



Obrázok 4.5 Grafické znázornenie topológie navrhovanej siete

4.7 Kalkulácia nákladov

Výstavba bezdrôtovej infraštruktúry musí rešpektovať zásadu kvality nad kvantitou. Pádny argumentom je bezpečnosť dát a účinná obrana voči prípadnému útoku na sieť, keďže šírenie rádiového signálu nemôžeme fyzicky ustrážiť. Progresívna technológia 4. generácie všetkým týmto podmienkam plne vyhovuje, dokonca poskytuje radu výhod a riešenie problémov, ktoré sa vyskytujú pri bežných WLAN.

Finančné možnosti firiem často limitujú vznikajúce projekty, ktoré sa tak uchýľujú k hľadaniu najlacnejšieho variantu na úkor kvality. Schodnou cestou môže byť práve správne podanie výhod a poukázanie na vysokú kvalitu, bezproblémový chod a trvácnosť riešenia. Navýšená cena projektu sa v priebehu niekoľkých rokov plne odzrkadlí v nižších nákladoch na prevádzku a servis zariadení.

Aplikácia najmodernejšej technológie naznačuje smerovanie firmy ako celku. Golf International spol. s r.o. neustále vylepšuje svoje moderné prevádzky golfového ihriska a hotelu, preto je pre nich tento variant ideálnym riešením so zárukou dlhoročnej spokojnosti a kvality. Aj v situácii, kedy sa na trhu objaví ešte výkonnejšie a kvalitnejšie riešenie, môžeme s prehľadom tvrdiť, že projekt implementácie WLAN štvrtej generácie je ideálnym riešením pre multifunkčný objekt typu biznis – relax – zábava- administrácia.

Položka	MJ	Počet	Bez DPH	
			cena/MJ	cena celkom
Switch EXSW 1200	ks	1	7 231,00 €	7 231,00 €
AP EXRP 40	ks	5	558,00 €	2 790,00 €
Kábel UTP, lanko, cat. 5e	m	305	0,26 €	78,00 €
Konektor RJ45 + krytka	ks	20	0,22 €	4,40 €
Inštalácia a zaškolenie	hod	4	33,00 €	132,00 €
Zľava na hardvér Extricom			15%	1 503,15 €
Spolu bez DPH				8 727,85 €
DPH				1 658,29 €
Spolu				10 386,14 €

Tabuľka 4.1 Náklady na realizáciu

Kalkulácia nákladov (Tabuľka 4.1) zachycuje všetky položky potrebné k realizácii projektu a nezahŕňa ceny doplnkového vybavenia tj. RADIUS server. Zľavu vo výške 15% poskytuje dodávateľ zariadení spoločnosti Extricom a to za odber uceleného riešenia od autorizovaného dodávateľa aj s montážou a predvedením.

Riziká a nástrahy sa nevyhýbajú ani tým najlepším projektom. Konkrétnejšie u nášho návrhu závisí cena zariadení EXSW 1200 a EXRP 40 od vývoja kurzu eura voči českej korune. Ten za obdobie 27.01 – 13.4 2010 zaznamenával posilnenie pozície českej koruny. Nepriaznivý dopad na euro má aj situácia, týkajúca sa grécka a jeho ekonomického stavu. Eurozóna ako celok tým prichádza o stabilitu eura, ktoré za obdobie 30.04 – 15.05 ešte viac oslabuje voči ostatným menám. Preto je otázne, čo prinesie budúcnosť a kedy bude najvýhodnejšie uskutočniť nákup spomínaných zariadení. Pri pohybe kurzu českej meny, napríklad o 1,- Kč v náš prospech, spoločnosť ušetri na nákupe približne 400 €.

ZÁVER

Vlastný návrh implementácie bezdrôtovej technológie vo firemnom prostredí, ktoré nie je jednotvárne ale vyžaduje multifunkčnosť, zahŕňa použitý systém WLAN štvrtej generácie. Eliminuje všetky doposiaľ známe problémy, ako prechod medzi nadväzujúcimi AP, vzájomné rušenie frekvencií, nutnosť napájania AP pomocou adaptéra a pokrytie jedného miesta viacerými sieťami iba s jedným AP. Konkurenčné technológie riešia uvedené nedostatky zväčša prostredníctvom softvéru, čo nie vždy prináša požadovaný efekt a často sú tieto varianty komplikované na správu systému. Nespornou výhodou je management celej rozsiahlej siete vykonávaný za pomoci jediného zariadenia – centrálného prvku EXSW-1200.

Prínosom riešenia pre spoločnosť Golf International s. r. o. bude všeobecná spokojnosť zo strany zamestnancov a hostí, plynúca zo stability a kvality bezdrôtovej siete v hoteli a príľahlých administratívnych priestoroch. Zvýšenie produktivity zamestnancov vďaka ich priestorovej mobilite prinesie firme mierne navýšenie príjmov. Vyššie vstupné náklady technológie sa postupne, aj za pomoci iných faktorov ako úspora elektrickej energie, vo svojej podstate znížia a dosiahnu úroveň bežného riešenia firemnej bezdrôtovej siete.

Súčasnosť poukazuje na potrebu kvalitného zabezpečenia všetkých podnikových sietí, kde sa prenášajú informácie. Tie v sebe nesú čoraz väčšie hodnoty, ktoré je potrebné chrániť. Môžeme sa stretnúť s názorom, že nie je vhodné používať bezdrôtové technológie v korporátnom prostredí. Za posledných 10 rokov však vývoj priniesol kvalitné a doposiaľ neprelomené techniky šifrovania dát AES, ktoré výrazne zvyšujú bezpečnosť dát. Aj naše riešenie sa sústreďuje na túto problematiku a zavádza najmodernejšie ochranné a autentizačné prvky.

Stále značný počet firiem, hlavne stredných a menších, chráni svoje bezdrôtové siete neadekvátnym spôsobom a neuvedomuje si potenciál prípadných únikov dát.

ZOZNAM POUŽITEJ LITERATÚRY

- (1) BRISBIN, Shelly. *Wi-fi: postavte si svou vlastní wi-fi síť*. 1.vyd. Praha: Neocortex, 2003. 248 s. ISBN 80-86330-13-3.
- (2) REHÁK, Dušan, *Satelitná komunikácia a služby umožňujúce mobilitu v TCP/IP*. [online]. 2004 [cit. 2010-05-04]. Dostupné z: <<http://www.fi.muni.cz//usr/staudek/rehak/diplomovka.html>>.
- (3) PUŽMANOVÁ, Rita. *Bezdrátové optické sítě*. [online]. 2003 [cit. 2010-05-05]. Dostupné z: <<http://www.lupa.cz/clanky/bezdratove-opticke-site/>>.
- (4) *Get IEEE 802®*. [online]. 1999 [cit. 2010-05-05]. Dostupné z: <<http://standards.ieee.org/getieee802/portfolio.html>>.
- (5) BARKEN, Lee. *Wi-Fi: jak zabezpečit bezdrátovou síť*. 1.vyd. Brno: Computer Press, 2004. 174 s. ISBN 80-251-0346-3.
- (6) KÖHRE, Thomas. *Stavíme si bezdrátovou síť Wi-fi*. 1.vyd. Brno: Computer Press, 2004. 296 s. ISBN 80-251-0391-9.
- (7) *List of WLAN channels*. [online]. 2009 [cit. 2010-05-05]. Dostupné z: <http://en.wikipedia.org/wiki/List_of_WLAN_channels>.
- (8) SIMANDL, Martin. *IEEE 802.11n — Jak na rychlé Wi-Fi doma i venku*. [online]. 2010 [cit. 2010-05-06]. Dostupné z: <<http://pctuning.tyden.cz/hardware/site-a-internet/16921?start=3>>.
- (9) WIRELESSHD, LLC. *About*. [online]. 2010 [cit. 2010-05-06]. Dostupné z: <<http://www.wirelesshd.org/about/>>.
- (10) WIGIG ALLIANCE. *Specifications*. [online]. 2010 [cit. 2010-05-06]. Dostupné z: <<http://wirelessgigabitalliance.org/specifications/>>.
- (11) VACULÍN, Ján. *Revoluce v bezdrátech! WiFi 4. generace*. [online]. 2009 [cit. 2010-05-07]. Dostupné z: <http://www.intelek.cz/art_doc-D7A489A18B634F84C12575550053ECAE.html>.
- (12) ZANDL, Patrick. *Bezdrátové sítě WiFi : praktický průvodce*. 1.vyd. Brno: Computer Press, 2003. 190 s. ISBN 80-7226-632-2.
- (13) IMAI, H. *Wireless communications security*. Nordwood: Artech House. 2006. 179 s. ISBN 1-58053-520-8.
- (14) DSL.SK. *Útok na WiFi WPA zlepšený*. [online]. 2009 [cit. 2010-05-07]. Dostupné z: <http://www.dsl.sk/article.php?article=7975&title=>>.

- (15) HG-COMPUTERS. *Wi-Fi*. [online]. 2010 [cit. 2010-05-010]. Dostupné z: <<http://www.hg-computers.sk/WiFitypi.pdf>>.
- (16) BRAUN, Lukáš. *Bezpečnosť WLAN u firiem v Európe je stále nízka*. [online]. 2009 [cit. 2010-05-11]. Dostupné z: <<http://www.zive.sk/bezpecnost-wlan-u-firiem-v-europe-je-stale-nizka/sc-4-a-282124/default.aspx>>.
- (17) ČSÚ. *IT v podnikách ČR - výsledky za leden 2009*. [online]. 2010 [cit. 2010-05-12]. Dostupné z: <[http://www.czso.cz/csu/redakce.nsf/i/1_it_v_podnicich_cr_vysledky_za_leden_2009/\\$File/1_it_podniky_cz_2009.xls](http://www.czso.cz/csu/redakce.nsf/i/1_it_v_podnicich_cr_vysledky_za_leden_2009/$File/1_it_podniky_cz_2009.xls)>.
- (18) VISIBLE BRAND. *Aktuálna ponuka*. [online]. 2010 [cit. 2010-05-13]. Dostupné z: <http://www.golftatry.sk/sk/aktualna_ponuka-type-hotel-id-102.html>.
- (19) EXTRICOM. *Datasheet: EXSW-1200 Wireless LAN Switch*. [online]. 2010 [cit. 2010-05-14]. Dostupné z: <http://www.extricom.com/media/KDxB_extricom_ds_exsw1200_v1.pdf>.
- (20) EXTRICOM. *Datasheet: EXRP-20/40 Access Point*. [online]. 2010 [cit. 2010-05-14]. Dostupné z: <http://www.extricom.com/media/nfe-_extricom_ds_ultrathinexrp20_40%20v1.pdf>.

ZOZNAM OBRÁZKOV

Obrázok 2.1 Grafické znázornenie rozdelenia frekvencií (2).....	11
Obrázok 2.2 Referenčný model OSI.....	14
Obrázok 2.3 Problém skrytého uzlu	16
Obrázok 2.4 Rozloženie kanálov v pásme (7)	18
Obrázok 2.5 MIMO technológia 2x2 (8)	18
Obrázok 2.6 Logo štandardu Wireless HD.....	20
Obrázok 2.7 Logo Wireless Gigabit Alliance.....	21
Obrázok 2.8 Možné využitie blanketov siete.....	22
Obrázok 2.9 Grafické znázornenie ad-hoc	23
Obrázok 2.10 Grafické znázornenie infraštruktúry	24
Obrázok 2.11 Základné typy antén (12)	27
Obrázok 2.12 Autentizácia podľa 802.1X (12).....	32
Obrázok 3.1 Graf zabezpečenia ICT v podnikoch (2009) (17)	34
Obrázok 3.2 Hotel International ***** (18).....	35
Obrázok 4.1 Dvanásť portový switch pre AP (19)	39
Obrázok 4.2 Štvorrádiový AP 802.11a/b/g (20)	40
Obrázok 4.3 Umiestnenie AP v administratívnej zóne.....	41
Obrázok 4.4 Umiestnenie AP v hotelovej časti	42
Obrázok 4.5 Grafické znázornenie topológie navrhovanej siete	45

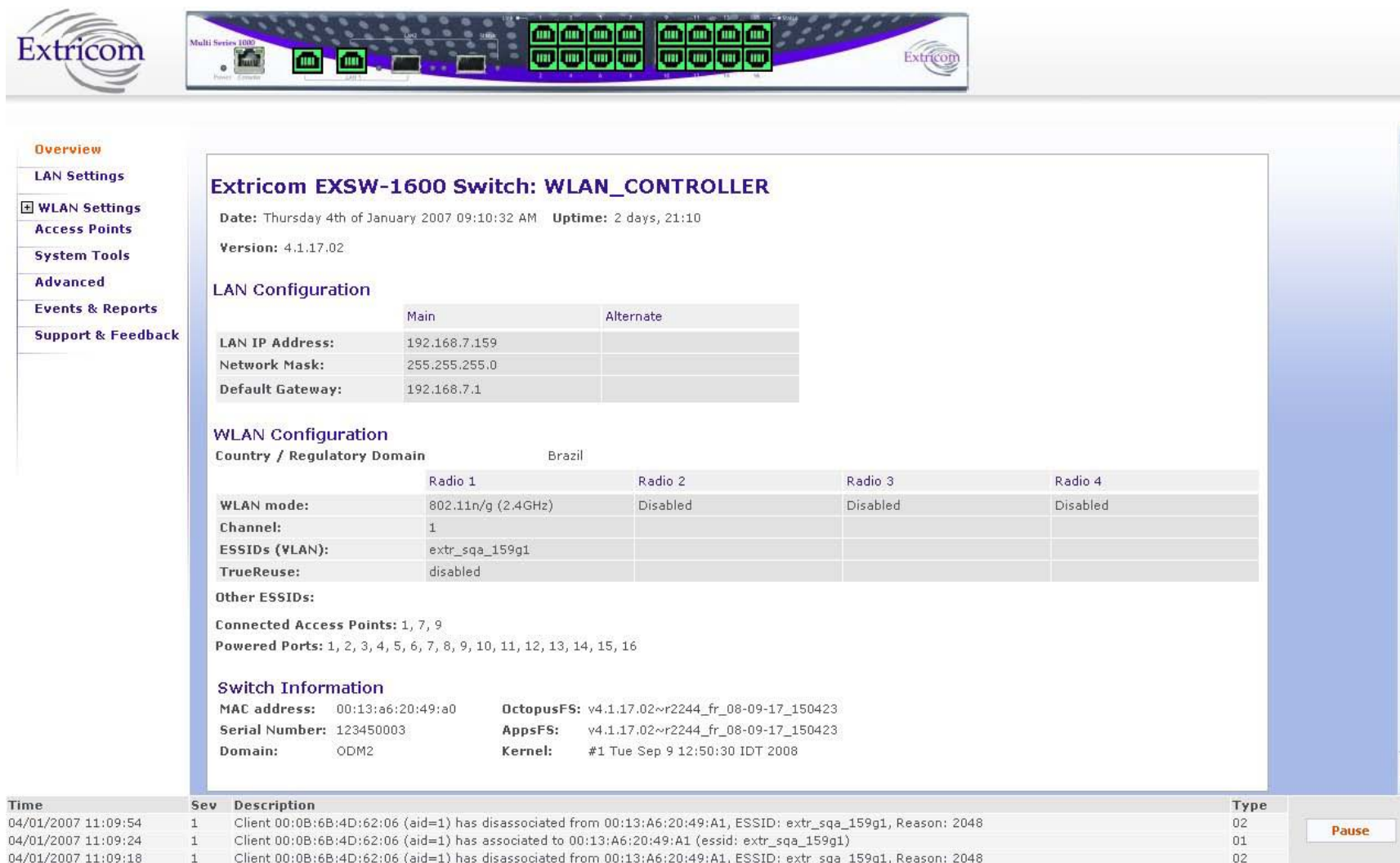
ZOZNAM TABULIEK

Tabuľka 4.1 Náklady na realizáciu	46
---	----

ZOZNAM PRÍLOH

- Príloha 1 Snímok obrazovky konfigurácie EXSW-1200 : Úvodná obrazovka so zobrazením stavu celej WLAN
- Príloha 2 Snímok obrazovky konfigurácie EXSW-1200 : Nastavenie hodnôt u jednotlivých SSID
- Príloha 3 Snímok obrazovky konfigurácie EXSW-1200 : Nastavenie RADIUS servera
- Príloha 4 Snímok obrazovky konfigurácie EXSW-1200 : Konfigurácia rádii jednotlivých AP

Príloha 1 Snímok obrazovky konfigurácie EXSW-1200 : Úvodná obrazovka so zobrazením stavu celej WLAN



The screenshot displays the configuration page for an Extricom EXSW-1600 Switch acting as a WLAN controller. The interface includes a navigation menu on the left and a main content area with various configuration sections.

Navigation Menu:

- Overview
- LAN Settings
- WLAN Settings (selected)
- Access Points
- System Tools
- Advanced
- Events & Reports
- Support & Feedback

Extricom EXSW-1600 Switch: WLAN_CONTROLLER

Date: Thursday 4th of January 2007 09:10:32 AM Uptime: 2 days, 21:10
Version: 4.1.17.02

LAN Configuration

	Main	Alternate
LAN IP Address:	192.168.7.159	
Network Mask:	255.255.255.0	
Default Gateway:	192.168.7.1	

WLAN Configuration

Country / Regulatory Domain: Brazil

	Radio 1	Radio 2	Radio 3	Radio 4
WLAN mode:	802.11n/g (2.4GHz)	Disabled	Disabled	Disabled
Channel:	1			
ESSIDs (VLAN):	extr_sqa_159g1			
TrueReuse:	disabled			

Other ESSIDs:

Connected Access Points: 1, 7, 9
Powered Ports: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16

Switch Information

MAC address:	00:13:a6:20:49:a0	OctopusFS:	v4.1.17.02~r2244_fr_08-09-17_150423
Serial Number:	123450003	AppsFS:	v4.1.17.02~r2244_fr_08-09-17_150423
Domain:	ODM2	Kernel:	#1 Tue Sep 9 12:50:30 IDT 2008

Event Log:

Time	Sev	Description	Type
04/01/2007 11:09:54	1	Client 00:0B:6B:4D:62:06 (aid=1) has disassociated from 00:13:A6:20:49:A1, ESSID: extr_sqa_159g1, Reason: 2048	02
04/01/2007 11:09:24	1	Client 00:0B:6B:4D:62:06 (aid=1) has associated to 00:13:A6:20:49:A1 (essid: extr_sqa_159g1)	01
04/01/2007 11:09:18	1	Client 00:0B:6B:4D:62:06 (aid=1) has disassociated from 00:13:A6:20:49:A1, ESSID: extr_sqa_159g1, Reason: 2048	02

Pause

Príloha 2 Snímok obrazovky konfigurácie EXSW-1200 : Nastavenie hodnôt u jednotlivých SSID

The screenshot displays the configuration interface for an Extricom EXSW-1200 switch. The interface is divided into several sections:

- Header:** Features the Extricom logo on the left and a top navigation bar with tabs for "ESSID Settings", "MAC ACL", and "RADIUS".
- Left Sidebar:** Contains a navigation menu with categories like "Overview", "LAN Settings", "WLAN Settings", "Access Points", "System Tools", "Advanced", "Events & Reports", and "Support & Feedback". Under "WLAN Settings", "ESSID Definition" is selected.
- Main Content Area:**
 - Select ESSID:** A list box shows "Octopus_1" (selected) and "Octopus_2". Buttons for "Rename" and "Delete & Save" are present.
 - New ESSID:** A text input field with an "Add & Save" button.
 - ESSID Octopus_1 Settings:** A grid of configuration options:

Allow Default ESSID	<input checked="" type="checkbox"/>	AeroScout Support	<input type="checkbox"/>
Display ESSID in Beacon	<input checked="" type="checkbox"/>	MAC Authentication	<input type="checkbox"/>
Allow Store & Forward	<input type="checkbox"/>	Beacon Rate Control	Normal
Allow Inter-ESS Forward	<input type="checkbox"/>	In Band Management	<input type="checkbox"/>
Enable Multicast	<input type="checkbox"/>	Captive Portal	<input type="checkbox"/>
Enable ARP Caching	<input type="checkbox"/>	VLAN (1-4094)	none
MAC ACL	<input type="checkbox"/>	Disassociation Timeout (0-3600)	3600
MAC ACL Mode	Whitelist	DTIM	3
802.11d Support	<input type="checkbox"/>	EAPOL Start Only	<input type="checkbox"/>
 - Encryption:** A section with a "WPA2 Only" checkbox.
 - Buttons:** "Save" and "Cancel" buttons are located on the right side of the settings area.
- Bottom Panel:** A log table with columns "Time", "Sev", "Description", and "Type".

Time	Sev	Description	Type
Sep 13 2009 19:51:08	1	APS: 5 have been connected	13

 A "Pause" button is located to the right of the log table.

Príloha 3 Snímok obrazovky konfigurácie EXSW-1200 : Nastavenie RADIUS servera

The screenshot displays the configuration interface for an Extricom EXSW-1200 switch. At the top, there is a banner image of the switch hardware with the Extricom logo on the left and right. Below the banner is a navigation menu on the left side with the following items: Overview, LAN Settings, WLAN Settings (expanded), ESSID Definition, Radios, Assignments, Access Points, System Tools, Advanced, Events & Reports, and Support & Feedback.

The main configuration area is titled "RADIUS" and contains a table for defining RADIUS servers. The table has columns for Server Name, Server Address, Server Password, Server Port, Server Timeout, and Remove. There are two rows in the table, with the first row populated with the following values:

	Server Name	Server Address	Server Password	Server Port	Server Timeout	Remove
1.	RADIUS1	192.168.0.1	●●●●●●	1812	30 secs.	<input type="checkbox"/>
2.						

A "Save" button is located in the top right corner of the RADIUS configuration area. At the bottom of the interface, there is a log table with the following columns: Time, Sev, Description, and Type. The log contains three entries:

Time	Sev	Description	Type
Jan 01 2007 16:39:31	2	APs 25 have been disconnected	14
Jan 01 2007 16:39:31	2	Radio 1 is not functioning in access points: 25	65
Jan 01 2007 16:39:31	2	Radio 4 is not functioning in access points: 15, 23	65

A "Pause" button is located to the right of the log table.

Priloha 4 Snímok obrazovky konfigurácie EXSW-1200 : Konfigurácia rádií jednotlivých AP

The screenshot displays the configuration page for the radio settings of an AP. The interface is divided into several sections:

- Navigation:** Overview, LAN Settings, WLAN Settings (ESSID Definition, **Radios**, Assignments), Access Points, System Tools, Advanced, Events & Reports, Support & Feedback.
- Radio Settings:**
 - Select Country: Brazil
 - Radio 1: 802.11n (2.4GHz), Channel 1, Max Retries 5, 20/40MHz, Mixed, 400 nSec, MCS 12.
 - Radio 2: Disabled, Max Retries 5, 20/40MHz, Mixed, 800 nSec, MCS 4.
 - Radio 3: Disabled, Max Retries 5, 20/40MHz, Mixed, 800 nSec, MCS 4.
 - Radio 4: Disabled, Max Retries 5, 20/40MHz, Mixed, 800 nSec, MCS 4.
- Rates (Mbps):** A table showing the status of various data rates for each radio.
- Log:** A table at the bottom showing system events.

Rate (Mbps)	Radio 1	Radio 2	Radio 3	Radio 4
54Mbps	Optional	Disabled	Disabled	Disabled
48Mbps	Optional	Disabled	Disabled	Disabled
36Mbps	Optional	Disabled	Disabled	Disabled
24Mbps	Basic	Disabled	Disabled	Disabled
18Mbps	Optional	Disabled	Disabled	Disabled
12Mbps	Basic	Disabled	Disabled	Disabled
11Mbps	Disabled	Disabled	Disabled	Disabled
9Mbps	Optional	Disabled	Disabled	Disabled
6Mbps	Basic	Disabled	Disabled	Disabled
5.5Mbps	Disabled	Disabled	Disabled	Disabled
2Mbps	Disabled	Disabled	Disabled	Disabled
1Mbps	Disabled	Disabled	Disabled	Disabled

Time	Seq	Description	Type
D4/D1/2007 11:24:38	1	Client DD:08:6B:4D:62:D6 (aid=1) has disassociated from DD:13:A6:2D:49:A1, ESSID: ext_sqa_159g1, Reason: 2D48	D2
D4/D1/2007 11:24:09	1	Client DD:08:6B:4D:62:D6 (aid=1) has associated to DD:13:A6:2D:49:A1 (essid: ext_sqa_159g1)	D1
D4/D1/2007 11:22:52	1	Client DD:08:6B:4D:62:D6 (aid=1) has disassociated from DD:13:A6:2D:49:A1, ESSID: ext_sqa_159g1, Reason: 2D48	D2