Bezpečnosť informačného systému podniku

Company Information System Security

Bc. Lukáš Nemec

Diplomová práca
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Lukáš NEMEC**
Osobní číslo:	**A10932**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Bezpečnost informačního systému podniku**

Zásady pro vypracování:

1. **Proveďte klasifikaci sítí.**
2. **Uveďte dělení standardů a jednotlivých sdílených pásem.**
3. **Analyzujte otázky bezpečnosti objektu.**
4. **Vypracujte návrh řešení bezdrátové sítě pro daný komplex budov.**
5. **Řešte jeho napojení na bezpečnostní systém.**
6. **Systém vyhodnoťte z pohledu zvoleného řešení, bezpečnosti.**
7. **Proveďte cenové vyhodnocení projektu a vypočtěte základní základní dobu návratnosti.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **Flickenger,R.: Building Wireless Comunity Networks. vyd. Boston: O?Reilly, 2003. 363 s. ISBN 0-596-00204-1**
2. **Quelet, E., Padjen, R., Pfund, A., Fuller, R., Blankenship, T.: Building a Cisco Wireless LAN. Vyd. USA: Syngress Publishing, 2002. 410 s.ISBN 0080476244**
3. **Everts, T., Audeh,M.: The Wireless LAN Book for Enterprises. vyd. Canada: Trapeze Networks, 2003. 220 s. ISBN 700-9501-0001**
4. **Barken L.: Ako zabezpečit sít WiFi. vyd. Brno: Computer Press, 2004, 176 s. ISBN 80-251-0346-3**
5. **Pužmanova, R.: Bezpečnost bezdrátové komunikace. vyd. Brno: Computer Pres, 2005, 184 s. ISBN 80-251-0791-4**
6. **Pužmanova, R.: Širokopásmový internet: Prístupové a domáci síte. vyd. Brno: Computer Pres, 2004. 384 s. ISBN 8025101398**

Vedoucí diplomové práce: **Ing. Radek Šilhavý, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **24. února 2012**

Termín odevzdání diplomové práce: **15. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cieľom tejto diplomovej práce je snaha o poukázanie na nebezpečenstvá podcenenia ochrany informačného systému podniku z pohľadu prenosových médií vo forme bezdrôtových sieti.

Podáva prehľad o dostupných bezdrôtových technológiách, systémoch a službách používaných v súčasnej dobe na zabezpečenie mobility. Úvod venujem klasifikácii sietí WPAN, WLAN, WWAN, WMAN, deleniu štandardov a jednotlivým zdieľaným pásmam. Ďalej sa venujem riešeniu a popisu otázok bezpečnosti. Výsledkom tejto práce je zhodnotenie použiteľnosti bezdrôtových technológii pre určitý komplex budov. (Architektúra, pokrytie, hardware, bezpečnosť, cena, atď.)

Kľúčové slova: WiFi, IEEE 802.11, WLAN

ABSTRACT

The aim of this diploma work is an effort to highlight the dangers of undermining the protection of business information system in terms of transmission media in the form of wireless networks.

The work contains the overview of the available wireless technologies, systems and services used in today's world for securing mobility. The first part of the work is dedicated to classification of WPAN, WLAN, WWAN,WMAN networks, followed by the division of standards and individual shared zones. In the second part I explore the security solutions and overall description of the topic. This is the integral part of the work. The outcome of this work is the evaluation of the usage and security of wireless network used for specific complex of buildings (the overall architecture, coverage, hardware, security, etc.).

Keywords: WiFi, IEEE 802.11, WLAN

Poďakovanie

Chcem sa poďakovať všetkým, ktorých rady a pripomienky prispeli k spracovaniu tejto diplomovej práce, za odborné konzultácie a poskytnuté informácie vedúcemu mojej diplomovej práce, ktorým je p. Ing. Radek Šilhavý,Ph.D. a oponent p. Ing. Ivan Kiss. Poďakovanie chcem venovať aj firme, v ktorej pracujem za možnosť nahliadnuť na fungovanie systému a plánov budov, ktoré boli v tejto práci použité

Prehlasujem, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

1 ÚVOD

1.1 Predslov

Bezpečnosť informačných systémov v podniku je jedným zo základných predpokladov stability a neohrozeného rastu. Ochrana firiem sa stala aktuálnou témou vďaka zvyšujúcim sa útokom hackerov. Dynamický vývoj technológií, globálne prepojené systémy a kompletná komunikácia cez internet predstavujú vysoké riziko úniku informácií a zneužitia zraniteľných miest.

V tejto diplomovej práci sa zameriam najme na bezpečnosť informačného systému podniku z pohľadu prenosových médií vo forme bezdrôtových sieti, ktoré predstavujú moderný trend v mobilnej hlasovej i dátovej komunikácií. Mobilita, flexibilita, prispôsobiteľnosť a úspora nákladov sú nezanedbateľné výhody týchto riešení. Na druhej strane so sebou existencia bezdrôtovej siete prináša niekoľko nevýhod. Relatívne nízka prenosová rýchlosť nie je zásadný problém, avšak je nutné počítať s ňou. Oveľa závažnejšie je bezpečnostné riziko.

Na rozdiel od ethernetových sietí, kde sú dáta aspoň sčasti chránené, pri bezdrôtovej komunikácií dáta lietajú voľne vzduchom a fyzicky nie je možné obmedziť ich prenosovú trasu. Pri neodbornom nastavení môže ísť o dvere dokorán otvorené útočníkom z ulice . V tomto prípade doslova, pretože presah signálu za múry kancelárií dovoľuje útok napríklad z auta zaparkovaného pri budove. Táto problematika je preto veľmi aktuálna a zaoberajú sa ňou rôzne skupiny a organizácie (napr.IEEE - *Institute of Electrical and Electronics Engineers*), ktoré neustále prijímajú nové štandardy z oblasti bezpečnosti.

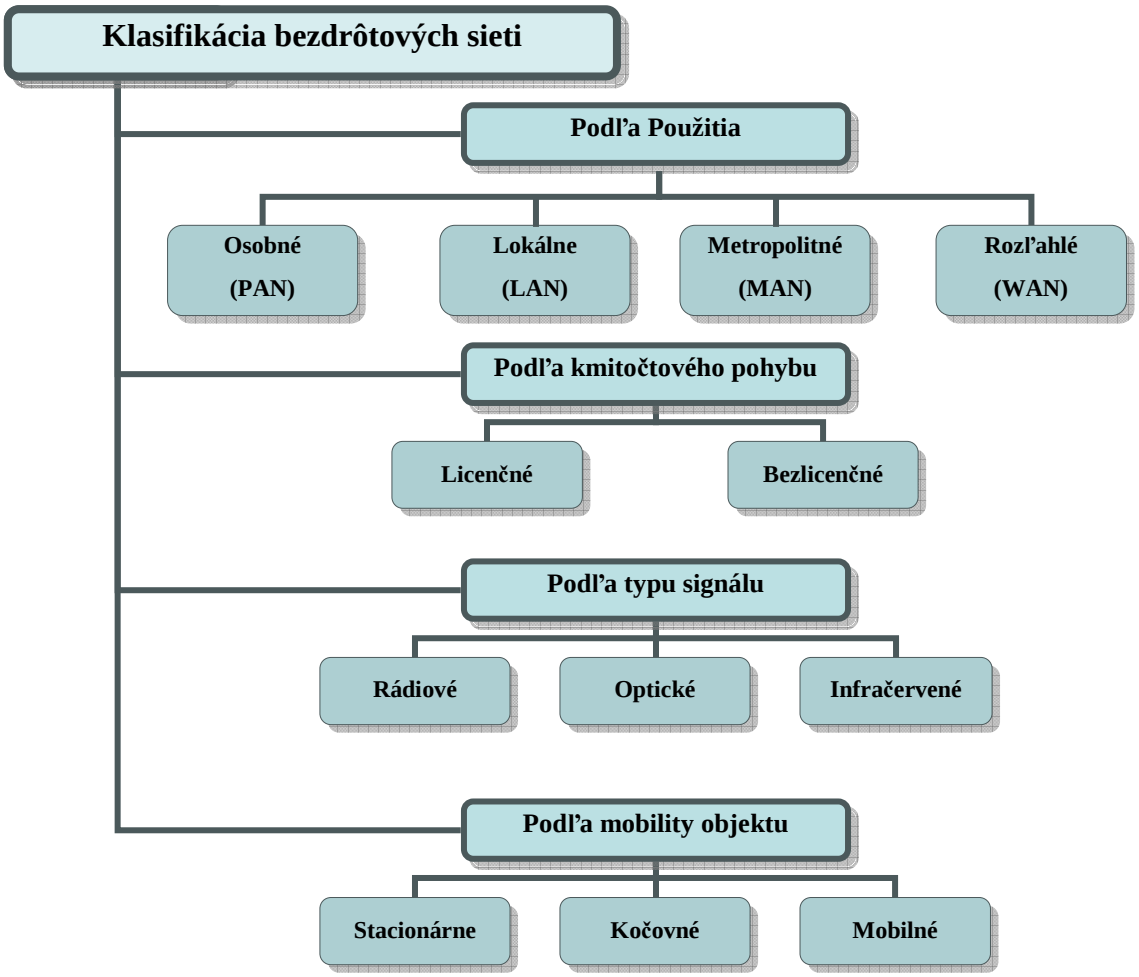
1.2 Cieľ

Cieľom tejto diplomovej práce je snaha o poukázanie na nebezpečenstvá podcenenia ochrany informačného systému podniku z pohľadu prenosových médií vo forme bezdrôtových sieti. Ďalším cieľom je návrh alternatívneho riešenia pre určitý komplex budov a jeho technické, ekonomické a bezpečnostné zhodnotenie. Pre tento návrh je ale najskôr nutné podať prehľad o dostupných bezdrôtových technológiách, ktoré sú dnes, alebo čoskoro budú aktuálne.

I. TEORETICKÁ ČASŤ

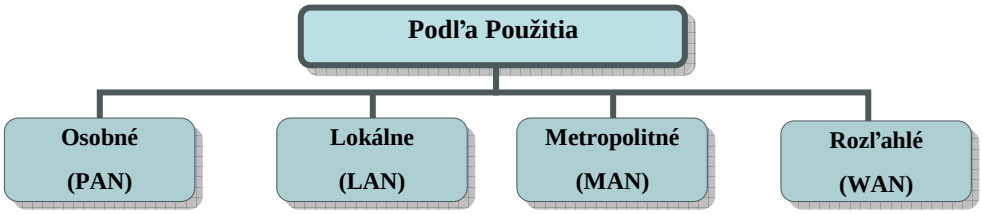
2 KLASIFIKÁCIA BEZDRÔTOVÝCH SIETI

Bezdrôtové siete a systémy sú alternatívou drôtových (metalických, optických) systémov. Poskytujú väčšiu flexibilitu a mobilitu ale oproti drôtovým systémom majú sčasti obmedzenú prenosovú kapacitu a často sa môžeme stretnúť i s ďalšími špecifickými problémami, ako napríklad prenos v bezlicenčnom pásme. Širokopásmový bezdrôtový prístup (BWA) predstavuje moderný prostriedok pre vytvorenie systémov pracujúcich na vyšších frekvenciách .Vďaka novým moduláciám a anténnym systémom už niektoré nové BWA systémy nepotrebujú priamu viditeľnosť.



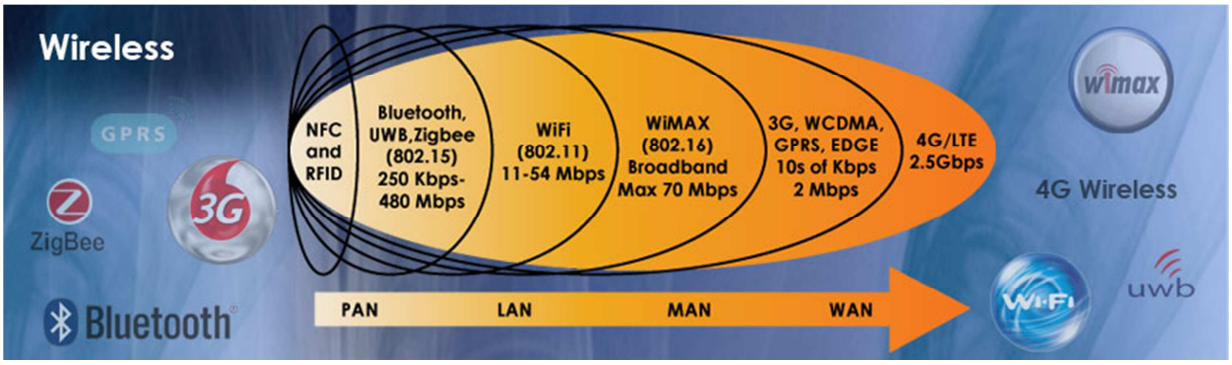
Obr.1Klasifikácia bezdrôtových systémov

2.1 Podľa použitia



Obr.2 Klasifikácia bezdrôtových systémov podľa použitia

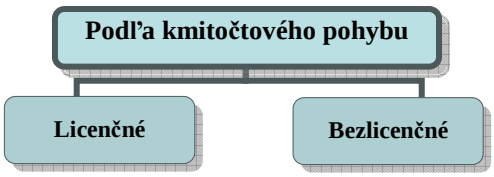
Delenie je zobrazené na obr.3 , kde sú uvedené konkrétne technológie, prenosové systémy a služby používané na prenos dát. Každý druh ma svoje špecifické vlastnosti. Siete LAN a MAN sa používajú najčastejšie v podnikových a mestských priestoroch, zatiaľ čo PAN sa používa najmä v domácich sieťach. WAN predstavujú mobilné 2G, 3G a najnovšie 4G siete. (Podrobná klasifikácia bezdrôtových sietí podľa použitia, je rozobratá v kapitole *3.1*, *3.2*, *3.3* a *3.5*)



Obr.3 Podrobné delenie bezdrôtových systémov podľa použitia

Zdroj: *http://www.einfochips.com*

2.2 Podľa kmitočtového pohybu

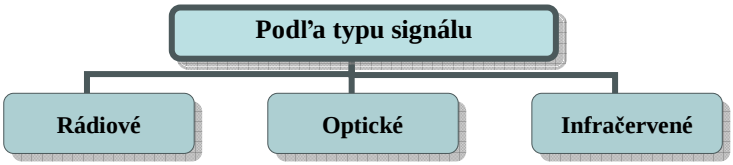


Obr.4 Klasifikácia bezdrôtových systémov podľa kmitočtového pohybu

Bezdrôtové systémy pracujú buď v licencovaných alebo bez licencovaných pásmach. Každé rádiové zariadenie používa pre prenos určíte pásmo, na ktoré je treba v prípade

bezlicenčných pásem generálne povolenie vydávané určitým regulačným úradom. Na Slovensku je to Telekomunikačný úrad SR. Pravidlá a pokyny týkajúce sa správy a licencií rádiových sietí sú verejne sprístupnené na stránkach. ***http://www.teleoff.gov.sk/***

2.3 Podľa typu signálu



Obr.5 Klasifikácia bezdrôtových systémov podľa typu signálu

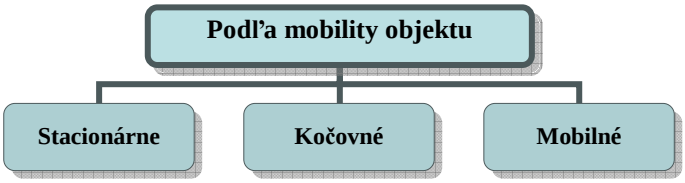
Rádiové siete patria medzi najčastejšie bezdrôtové siete. Majú rôzny dosah od jednotiek metrov až po desiatky kilometrov. Sú vhodné ako pre domáce siete, tak i pre širokopásmový prístup k internetu. Rádiový signál je schopný preniknúť rôznymi prekážkami, avšak niektoré zo sietí potrebujú priamu viditeľnosť (bez prekážok). Čím vyšší kmitočet je použitý, tím menší je dosah siete. Signál s nízkym kmitočtom sa šíri ako povrchová vlna, tzn. že sleduje zakrivenie zeme a môže docieliť značného dosahu. Signál o kmitočte jednotiek GHz sa šíri ako priama vlna a je obmedzená geometrickým (optickým) horizontom, preto je jeho dosah obmedzený priamou viditeľnosťou. Mikrovlnné technológie sú vhodné pre komunikáciu vo vnútornom ale i vonkajšom prostredí. Rádiové siete pracujú v rámci priestorových oblastí, v ktorých môžu stanice komunikovať (prostredníctvom základňových staníc alebo prístupových bodov).

Optické siete majú dosah od desiatok metrov až po jednotky kilometrov. Kvalita signálu je ale výrazné ovplyvnená priamou viditeľnosťou. Pokiaľ sa na ceste medzi optickými jednotkami vyskytne hmla alebo sneženie, môže dôjsť k veľkým stratám a často i k rozpojeniu spoja. Na druhej strane, tieto siete poskytujú vysokú prenosovú rýchlosť od jednotiek Mbit/s až po jednotky Gbit/s. Sú vhodným riešením pre podnikové siete pre komunikáciu medzi budovami.

Infračervené siete majú malý dosah, nedokážu prekonať prekážky, ako sú steny, stromy atď. Sú teda obmedzené na určitý priestor. Infračervené siete majú omnoho väčšiu šírku

pásma ako rádiové siete, nie sú limitované dostupným spektrom a taktiež nepodliehajú regulácii.

2.4 Podľa mobility objektu



Obr.6 Klasifikácia bezdrôtových systémov podľa mobility objektu

Stacionárne siete sú už podľa názvu siete pre komunikáciu v kľudovom stave, bez žiadneho presunu objektov. To znamená, že bezdrôtová technológia a jej vysielacia aj prijímacia časť je pevne rozmiestnená na vysielacích a prijímacích bodoch a v závislosti na použitej technológii, aby pri zmene polohy nedošlo k strate komunikácie.

Kočovné siete sú také, kde pri komunikácii je objekt v kľude (alebo v stave blížiacemu sa kľudu), avšak objekt sa medzi kľudovými stavmi pohybuje. Napríklad v aute ktoré sa pohybuje sa dá komunikácia použiť pri jeho zastavení napr. na čerpacej stanici, parkovisku atď.

Mobilné siete sú s plnou podporou mobilných komunikujúcich objektov. To znamená, že pri ich používaní nezáleží, či je objekt v kľude, alebo v pohybe.

3 DELENIE STANDARDOV A ZDIELANYCH PASEM

3.1 Bezdrôtové siete WPAN

WPAN sú pre pomerne krátky dosah využívané na špecifické aplikácie, kde je zbytočné alebo dokonca na škodu používať technológie s väčším dosahom. Prehľad detailov WPAN je stručné zobrazený v **Tab.1**.

3.1.1 Bluetooth 802.15.1

Bluetooth je rádiová technológia určená pre bezdrôtovú komunikáciu v rámci osobných sietí, na prenos hlasu, dát i videa. Túto technológiu vyvíja a spravuje už od roku 1998 spoločnosť SIG. Štandard Bluetooth bol prijatý normalizačným inštitútom IEEE ako norma pre osobné siete pod označením IEEE 802.15.1. Pôvodný štandard bol vo verzii 1.1 a poskytoval maximálnu rýchlosť prenosu 1Mbit/s (reálna rýchlosť max. 720kbit/s). Postupom času boli do IEEE 802.15.1 zakomponované ďalšie verzie a to 1.2 a verzia 2.0. V súčasnej dobe Bluetooth 2.0 ponúka prenosovú rýchlosť 2.1 Mbit/s vďaka novozavedenej modulácii Π/4-DQPSK, čo má za následok predovšetkým tri až desaťkrát vyššiu rýchlosť a nižšiu spotrebu energie.

Najnovší prírastok do rodiny bluetooth pribudol len prednedávnom a nesie označenie bluetooth 3.0 High Speed (HS). Kľúčovú úlohu v tejto verzii osobnej siete je PAL (protocol adaptačnej vrstvy) 802.11, ktorý umožňuje rozhraniu prenos prostredníctvom WiFi. Ak aspoň jedna z dvoch komunikujúcich strán nedisponuje rozhraním vo verzii 3.0, proces prenosu dát sa bude realizovať pomocou pomalšieho režimu s nižšou prenosovou rýchlosťou. Maximálna dosiahnuteľná rýchlosť sa pohybuje na úrovni 24Mbit/s. Viac informácií o Bluetooth a najnovšej verzii 3.0 je na www.bluetooth.com .

Obr.7 Bluetooth logo

Zdroj: ***http://www.bluetooth.com***

3.1.2 UWB 802.15.3

Ultra Wide Band je norma pre malé a zároveň rýchle bezdrôtové siete. V roku 2003 bola schválená základná verzia pod označením IEEE 802.15.3. Táto verzia pracuje v pásme 2,4 GHz a bez problémov dokáže spolupracovať s 802.11b/g, 802.15.1 a 802.15.4 technológiami. Ma malú spotrebu energie a podporuje rýchlosť až do 55Mbit/s. Systém v závislosti od prenosových podmienok volí jednu z piatich typov modulácie. (11, 22, 33, 44 a 55 Mbit/s) Využíva časové delenie TDMA (Time division multiple access).

Nadstavbová verzia 802.15.3a podporuje rýchlosť až do 110 Mbit/s do vzdialenosti 10m, a rýchlosť 480 Mbit/s do vzdialenosti 1m s využitím pásma o šírke 500 MHz a kmitočtového intervalu 3,1 GHz až 10,6 GHz. Toto široké spektrum odoláva voči rušeniu vďaka tomu, že rozkladá signál tak, aby výkon v každom jednotlivom pásme bol pod úrovňou možného rušenia iných úzkopásmových systémov.

Tab.1 Prehľad hlavných charakteristík bezdrôtových sietí WPAN

	Označenie	Kmitočet	Max. rýchlosť	Vznik normy
Bluetooth	802.15.1	2,4 GHz	24 Mbit/s	2002
UWB	802.15.3	3.1 – 10,6 GHz	100-500 Mbit/s	2007

3.2 Lokálne bezdrôtové siete WLAN

Na technológie patriace do tejto skupiny sa v rámci mojej práce zameriam najviac. WLAN zastupuje predovšetkým technológia WiFi, štandardy patriace do skupiny IEEE 802.11. Pokúsim sa priblížiť základné charakteristiky tohto štandardu. Ich kompletný popis by presiahol rozsah tejto práce. Údaje o pracovných frekvenciách a kanáloch sa často líšia v závislosti od kontinentu, ale základ tejto rodiny štandardov je rovnaký.

3.2.1 Špecifikácia WiFi (výhody / nevýhody)

WiFi je skratka pre “wireless fidelity“ a predstavuje spresnenie štandardu IEEE 802.11

Zariadenia s týmto označením zaručujú vzájomnú kompatibilitu.

Siete WiFi majú dve základné možnosti konfigurácie či topológie siete. V prvom prípade ide o siete spojené ako **ad-hoc** alebo inak **p2p** (peer-to-peer). Tu sú zariadenia spojené priamymi spojmi a komunikujú každý s každým. Väčšinou sa jedná o spojenie dvoch zariadení ale je možné ich takto spojiť aj viacej.

Druhú možnosť predstavujú siete tvoriace **Infraštruktúru.** Zostava siete tu obsahuje jeden alebo viac prístupových bodov (AP) jedného alebo viacerých klientov. AP vysiela svoj SSID (Service Set Identifier) prostredníctvom paketov nazývaných beacons (signály,majáky), ktoré sú vysielané každých 100ms rýchlosťou 1Mbps (najnižšia WiFi rýchlosť). To zaručuje, že klient prijímajúci signál z AP, môže komunikovať rýchlosťou aspoň 1Mbit/s. Na základe nastavení (napr. podľa SSID) sa klient môže rozhodnúť, či sa k AP pripojí. Ak sú napr. v dosahu klienta dva prístupové body s rovnakým SSID, klient sa podľa sily signálu môže rozhodnúť, ku ktorému AP sa pripojí. WiFi štandard úplne ponecháva pripojovacie kritéria na klienta.

Výhody:

- Využíva nelicencované rádiové pásmo (nie je potrebný súhlas miestnych úradov)
- Umožňuje vybudovať LAN bez káblov a tak zníži náklady na vybudovanie, či rozširovanie siete (výhodné v priestoroch, kde sa nemôžu použiť káble)
- Produkty WiFi sú na trhu široko dostupné
- WiFi siete podporujú roaming, vďaka ktorému sa mobilná klientská stanica (napr. laptop) môže presúvať od jedného prístupového bodu ku druhému bez straty spojenia súčasne s pohybom používateľa v budove alebo oblasti

Nevýhody:

- Wifi siete majú obmedzený dosah. Typický domáci smerovač môže mať dosah 45m v budovách a 90m mimo budovy
- Wifi štandardy používajú nelicencované pásmo 2,4Ghz, ktoré je preplnené inými zariadeniami napr. Bluetooth, mikrovlnne rúry, bezdrôtové telefóny alebo zariadenia na prenos video signálu

- Vysoká spotreba v porovnaní s inými štandardami znižuje životnosť baterií s spôsobuje prehrievanie zariadení
- Nesprávne nakonfigurované prístupové body môže záškodník využiť na anonymný útok

3.2.2 Klasifikácia noriem 802.11

Poznáme 4 druhy štandardných noriem WIFI: 802.11 a, b, g, n. (**Obr. 8**).

Tieto sú bližšie popísané v sekciách *3.2.5* až *2.3.8*.

Obr.8 Všeobecné normy WiFi sietí

Zdroj: *http://www.wifi.org*

Doplnkové normy :

Tab.2 Doplnkové normy	
802.11 e	Quality Of Service
802.11 h	Spectrum Manager 802.11a
802.11 i	Enhanced Security
802.11 d	Problém medzinárodnej použiteľnosti
802.11 f	Roaming medzi prístupovými bodmi

3.2.3 Dosah WiFi sietí

Dosah udávaný výrobcami sa pohybuje v okruhu 100m, avšak s použitím smerových antén

je možné dosah značne zvýšiť. Je treba dbať na to, aby nebol prekročený povolený vyžarovaný výkon. Pokiaľ nie je v priestore rušenie (viacstranne šírený signál, rušenie signálu inými systémami v rovnakom pásme, nepriama viditeľnosť, zlé počasie), je možné docieliť dosah až niekoľko kilometrov.

3.2.4 Štandard 802.11 (r.1997)

Najväčším problémom pôvodnej normy pre WLAN (802.11) bola nízka prenosová rýchlosť

Bol fyzicky riešený troma spôsobmi :

- prenos rádiových vĺn s frekvenciami v pásme od 2,4 do 2,4835GHz metódou priamo rozprestretého spektra (Direct Sequence Spread Spectrum, DSSS) – DSSS vysielač premenuje tok dát (bitov) na tok symbolov, kde každý symbol reprezentuje skupinu jedného či viacerých bitov. Požitá je modulačná technika QPSK.
  DSSS delí pásmo na 14 kanálov po 22MHz, ktoré sa čiastočne prekrývajú. Siete 802.11 založené na DSSS ponúkajú rýchlosť 1 až 2 Mbit/s.
- prenos rádiových vĺn s frekvenciami v pásme od 2,4 do 2,4835GHz metódou rozprestretého spektra s preskakovaním frekvencie (Frequency Hopping Spread Spectrum, FHSS) – FHSS vysiela jeden alebo viacero paketov dát po jednej frekvencií (preskakuje na inú frekvenciu a vysiela ďalej). Pásmo sa delí po 75 podkanálov, každý o jednom MHz. Siete 802.11 založené na FHSS ponúkajú rýchlosť 1 až 2 Mbit/s.
- prenos infračerveným žiarením (Diffused Infra red). Vyžaduje priamu viditeľnosť medzi vysielacím a prijímacím optickým prvkom. Tento variant lokálnej bezdrôtovej siete je preto značne obmedzený. Tato technológia je v súčasnosti prakticky nepoužívaná a preto sa v súčasnosti nepracuje na jej modernizácií.

3.2.5 Štandard 802.11a (r.1999)

Tento štandard je nekompatibilný s variantmi g, b a n. Je taktiež odlišný v mnohých technických parametroch. Kým varianty b,g,n sa veľmi rýchlo šírili v Európe, štandard 802.11a si získal uplatnenie najmä v USA.

Najväčší rozdiel je v použitom frekvenčnom pásme. 802.11a využíva pásmo 5GHz, ktoré je bezlicenčné ale technické riešenie spoľahlivých prenosov je pri tejto frekvencií náročnejšie. Výhoda spočíva najmä v tom, že oproti pásmu 2,4GHz je relatívne "čisté", je málo používané a preto aj takmer nenarušené.

Maximálna teoretická komunikačná rýchlosť tohto štandardu je 54Mbit/s. Používa OFDM moduláciu, pričom základný protokol tohto variantu je zhodný so základným štandardom IEEE 802.11.

Prenosové pásmo je delené na 54 sub-kanálov. Každý z nich je modulovaný niektorou z dostupných modulačných techník nižšej úrovne (BPSK,QPSK,QAM). Od použitej modulačnej techniky potom závisí prenosová rýchlosť.

Celková šírka prenosového pásma pre túto špecifikáciu je 20 MHz, delí sa do 12 neprekrývajúcich sa operačných kanálov.

3.2.6 Štandard 802.11 b (r. 1999)

Využíva frekvenčné pásmo 2,4 GHz, poskytuje však vyššie rýchlosti a to až do 11Mbit/s. Na ich dosiahnutie využíva doplnkové kódové kľúčovanie (Complemetary Code Keying, CCK) v rámci DSSS na fyzickej vrstve. Kódovanie CCK je istým variantom technológie CDMA, známej z moderných bezdrôtových sietí. Norma špecifikuje, že podľa momentálnej rušivosti prostredia sa dynamicky mení rýchlosť na nižšiu alebo naopak na vyššiu. Prenosové pásmo sa delí na 11 pracovných kanálov (5MHz pre každý).

Použiteľná rýchlosť sa udáva okolo 6Mbit/s pri použití TCP paketov. Dosah siete vo vnútri budov je okolo 30m a okolo 100m v extraviláne. Pri použití kvalitných smerových antén v nezarušenom priestore je možne dosiahnuť aj mnohokrát väčšie vzdialenosti.

3.2.7 Štandard 802.11 g (r.2003)

Využíva nové modulačné techniky OFDM (Orthogonal Frequency-division multiplexing). OFDM- jedná sa o metódu používanú pre generovanie a moduláciu signálu a viacej nosných signálov súčasne. Ide o multiplex, ktorý pracuje s rozprestretým spektrom (spread spectrum), kde je signál vysielaný na viacerých nezávislých frekvenciách, čo zvyšuje odolnosť voči interferencii. Jednotlivé subkanály sa vzájomne prekrývajú, čím sa dosiahne

oveľa efektívnejšie využitie frekvenčného spektra. Na jednej strane nám OFDM poskytuje rýchly multiplex, ale na druhej strane ma menší dosah a horšie vlastnosti v členitom teréne ako modulácia DSSS.

Tento štandard dokáže prepínať nielen medzi rýchlosťami, ale prepína aj modulačné techniky.

- Pre rýchlosť 6,9,12,18,24,36,48 a 54Mbit/s – OFDM
- Pre rýchlosť 5,5 a 11Mbit/s – CCK na DSSS
- Pre rýchlosť 1 a 2Mbit/s QPSK

Teoretická komunikačná rýchlosť až do 54Mbit/s

Štandardy 802.11 g neriešia ani problematiku prideľovania pásma podľa potrieb aplikácii a ani nezisťujú (QoS) kvalitu služieb, čo je dôležité najmä pre multimediálne prenosy. Problematická je i bezpečnosť komunikácie, pretože v prípade rádiovej komunikácie je mimoriadne jednoduché rádiový signál zachytiť a spracovať. Z týchto dôvodov sa IEEE zaoberá radom doplnkov k 802.11 (802.11d,e,f,h,i,j)

3.2.8 Štandard 802.11 n (r.2009)

Najnovšia generácia wifi sietí bola len pred nedávnom štandardizovaná a to pod označením 802.11n. Mnohoročné úsilie a množstvo draft verzii tejto technológie sa však objavovali už od roku 2004. Viac o priebehu štandardizácie viď. ***http://www.ieee.org .***

Celkový popis fungovania týchto štandardov je veľmi komplikovaný preto sa pokúsim iba o načrtnutie hlavných funkcií.

802.11n sa vyznačuje najmä zvýšenou rýchlosťou prenosu dát a to do rýchlosti 600MBit/s. Táto rýchlosť je dosiahnutá najmä využitím metód ako MIMO (*multiple-input and multiple-output)* a Channel bonding .

MIMO používa viacero antén pre vysielanie a príjem, pričom počet jednotlivých antén nemusí byt rovnaký. Dátový tok sa delí medzi antény. Signál sa nešíri len priamo, ale môže sa i odrážať od prekážok, pričom dráha signálu s odrazom je dlhšia, čo spôsobí, že signál príde s omeškaním.

Channel bonding je metóda vyznačujúca sa združovaním kanálov. Znamená to, že dva susedné kanály sa spoja do jedného širšieho kanálu. Zvýši sa tým priepustnosť na viac než dvojnásobok. Táto metóda sa však využíva iba v pásme 5GHz.

Štandard spätne podporuje a plne spolupracuje aj s verziami WiFi a,b,g. Používa dve možné pásma, a to najmä doporučené pásmo 5GHz a pásmo 2,4GHz. Pásmo 5GHz je doporučené hlavne kvôli možnosti využitia metódy Channel bonding a tým poskytuje väčšiu priepustnosť vďaka 40MHz kanálom. Toto širšie pásmo ma väčší počet neprekrývaných kanálov a menšie rušenie (žiadne bluetooth zariadenia, mikrovlnné rúry atď.).

Používaná je tu modulácia OFDM (pozri 2.3.7), ktorá pri použití 40Mhz kanálov dokáže využiť až 108 sub pásem.

Moduláciu zabezpečujú rôzne kombinácie kódovania ako BPSK, QPSK, 16-QAM a 64-QAM. Taktiež podporuje Qos štandard 802.11e.

Tab.3 Prehľad hlavných charakteristík bezdrôtových sieti WLAN

IEEE označenie	Kmitočet	Max. rýchlosť	Vznik normy
802.11	2,4 – 5 GHz	6 Mbit/s	1997
802.11a	5 GHz	54 Mbit/s	1999
802.11b	2,4 GHz	11 Mbit/s	1999
802.11g	2,4 GHz	54 Mbit/s	2003
802.11n	2,4 – 5 GHz	600 Mbit/s	2009

3.3 Metropolitné bezdrôtové siete WMAN

V skupine WMAN jednoznačné dominuje štandard WiMax 802.16. Tento štandard je veľmi vhodný pre profesionálne aplikácie, pretože pracuje v licencovaných pásmach, kde

by nemalo dochádzať k okolitému rušeniu, najviac má tento štandard veľmi vhodné prenosové parametre zaručujúce kvalitu služieb.

3.3.1 WiMax – 802.16

WiMAX (Worldwide Interoperability for Microwave Access - celosvetová interoperabilita pre mikrovlnný prístup) je nová širokopásmová rádiová technológia, využívaná na širokopásmový prístup na internet a ďalšie služby prístupné cez IP.

Prvá norma siete IEEE 802.16 bola vyvinutá v roku 2001. Bola určená pre frekvencie 10 – 66GHz a ponúkala kapacitu dát na fyzickej vrstve vo veľkosti pásma 268Mb/s. Táto norma však vyžadovala pri prenose priamu viditeľnosť a tak sa stala nepoužiteľnou pre nasadenie do reálneho používania.

Normy :

- IEEE802.16b– podporuje Qos a pracuje v pásme 5 až 6GHz.
- IEEE 802.16c-Je tu zrušená podmienka priamej viditeľnosti. Pásmo 2 – 11GHz

3.3.2 WiMax (výhody / nevýhody)

Výhody:

- Perspektívna technológia. Podpora hlavne u výrobcov koncových zariadení
- Podporuje pružné prideľovanie šírky pásma rádiových kanálov a ich opakované využívanie pre zvyšovanie kapacity siete
- I keď je priama viditeľnosť výhodná, systém môže pracovať aj v režime bez priamej viditeľnosti

Nevýhody:

- Značne vysoké zriaďovacie poplatky
- Pripojenie vyžaduje externú anténu
- Pomerne slabé pokrytie v rámci Slovenska. Komerčná ponuka je taktiež zatial slabá

3.3.3 IEEE 802.16d (r.2004)

Táto norma postavila základ služby WiMax. Norma umožňuje používať pásma v rozmedzí 2 – 11GHz, v praxi sa však využíva licencované pásmo 3,5GHz(v zámorí je to 2,4GHz). Nevyžaduje priamu viditeľnosť medzi vysielačom a prijímačom.

WiMax 802.16d na rozdiel od iných špecifikácií prenáša dáta v niekoľkých frekvenčných pásmach, vďaka čomu je minimalizovaná možnosť rušenia s inými rádiovými aplikáciami. V závislosti od voľby spektra sa mení dosah i maximálna rýchlosť prenosu.

Využitá modulácia OFDM ponúka možnosť dosiahnutia vysokých rýchlostí prenosu dát v sťažených podmienkach na vysielanie, či príjem signálu. OFDM rozdeľuje širokopásmový signál do 256 úzkopásmových kanálov, z ktorých každý prenáša asi 50Kb/s.Napriek tomu, že sú kanály blízko vo frekvenčnom pásme, nedochádza k prekrytiu, a tak neohrozí ich vzájomné rušenie. Pri OFDM prenose je tiež možné zanedbať vznik rušenia spôsobeného rôznymi trasami šírenia signálu či útlmu signálu vo vonkajšom prostredí.

Pri prenose dát pomocou technológie WiMax 802.16d sa dáta fyzicky prenášajú spôsobom označovaným ako FDD (Frequency-Division Duplex), čo znamená, že na prenos smerom od používateľa je použitá jedna frekvencia a ďalšia frekvencia sa používa na prenos v opačnom smere. Rozstup týchto pásem závisí od nosnej frekvencie.

Vo svete sa využíva aj spôsob označovaný ako TDD (Time Division Duplexing), ktorý na prenos v obidvoch smeroch využíva iba jednu frekvenciu, pričom príjem i vysielanie sú synchronizované v čase. V takomto prípade je šírka kanála 7MHz. Prístupový bod, označovaný aj ako bázová stanica vždy komunikuje v plnoduplexnom režime a pripojení klienti využívajú half duplex.

Obr.9 WiMax logo

Zdroj: *www.wimaxforum.org*

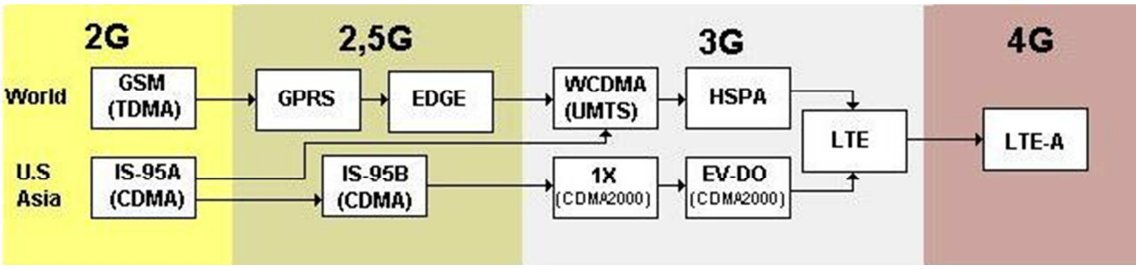
Najvyššia prenosová rýchlosť štandardu WiMax 802.16d pri frekvencii 3,5GHz je 12,699MB/s, pričom toto pásmo je vyhradené pre jeden sektor . Jedna bázová stanica môže pokrývať maximálne šesť sektorov, čo znamená, že maximálna prenosová rýchlosť

bázovej stanice sa pohybuje na úrovni 76,194 Mb/s. Pásmo môže byť rozdelené rôznymi spôsobmi. V závislosti od šírky kanála môže byť k jednej stanici pripojených až 750 ľudí, pričom každý z nich bude mať pridelené pásmo v šírke 0,5Mb/s.

WiMax 802.16d vie pracovať aj s moduláciami ako QAM,QPSK a BPSK. Je tomu tak kvôli schopnosti namodulovať viacej bitov do rovnakej šírky pásma a tým aj schopnosť rozpoznávať viacej stavov. Lenže ako sa s pribúdajúcou vzdialenosťou od BS zhoršuje SNR (pomer signál/šum), nie je možné rozoznať na prijímacej strane jednotlivé stavy spoľahlivo a preto sa používa „slabšia“ modulácia.

3.4 Rozľahlé bezdrôtové siete WWAN

Najväčším zástupcom rozľahlých bezdrôtových sietí WWAN sú siete mobilných operátorov založené na štandardoch GSM a UMTS. Pre prenos dát je v týchto sieťach možné využiť pomerne množstvo systémov a služieb. Jednotlivé technológie majú rozdielne parametre, predovšetkým ich oblasť pôsobnosti a dosah siete. Použitie jednotlivých technológií závisí od konkrétneho typu aplikácie. Existuje viacero štandardov, ktoré boli a sú vyvíjané decentralizovane na rôznych kontinentoch. V súčasnosti sa prejavujú snahy štandardy centralizovať (viď. Obr.10) a zabezpečiť čoraz vyššie rýchlosti a spoľahlivosť týchto sietí kdekoľvek na svete.



Obr.10 Vývoj rozľahlých bezdrôtových sietí WWAN

Zdroj: *http://www.ieee.org .*

3.4.1 GSM (Global System for Mobile communications)

GSM je označovaná ako sieť druhej generácie 2G (viď. Obr.10), a predstavuje prvý mobilný digitálny systém, ktorý je v súčasnosti najpoužívanejšou a teda najviac rozšírenou verziou rozľahlých sieti WWAN. Je to digitálny štandard určený k bezdrôtovej komunikácii. Pracuje na princípe FDMA/TDMA. FDMA (Frequncy Division Multiple Access) predstavuje mnohonásobný prístup do siete, kde sú jednotliví účastníci frekvenčne oddelení. Frekvenčné pásmo sa delí na kanály, ktoré sa prideľujú účastníkom a každý účastník má preto po celú dĺžku spojenia vyhradené pásmo rádiového kanálu . TDMA (Time Division Multiple Access) predstavuje mnohonásobný prístup do siete, v ktorej sú od seba účastníci oddelení v čase. Prenášaná informácia sa vkladá do časových intervalov (timeslotov).

Dĺžka každého timeslotu je približne 0,577 ms pri rozostupe nosných vĺn 200 khz. Kapacita systému je preto 8 alebo 16 užívateľov na kanál. Pri spomenutom rozostupe vĺn je možné poskytnúť od 124 do 174 kanálov. Prenosový výkon pre GSM 900 je maximálne 2W a pre GSM 1800 je to 1W .

GSM najčastejšie pracuje na spomínanej frekvencii 900/1800 MHz. Menej často je využitá frekvencia 400/450 MHz, ktorá bola zavedená len pre štáty, kde boli frekvencie 900/1800MHz už obsadené predchádzajúcou generáciou systémov.

Okrem najpoužívanejších hlasových hovorov poskytuje tento štandard aj veľmi obľúbenú službu SMS a iné funkcie ako napr. DTMF.

Prenos dát je tu riešený pri veľmi nízkych rýchlostiach a to iba do 9,6 kbps, čo sa postupným vývojom a príchodom služieb ako GPRS a EDGE napravilo.

3.4.1.1 SMS (Short Message Service)

SMS alebo krátke textové správy je taktiež možné použiť na prenos dát. Pri prenose sa využívajú signalizačné kanály namiesto hovorových. Poskytujú nám dĺžku 160 znakov. Pri prenose sa môže vyskytnúť problém ak príjemca nie je schopný vyzdvihnúť správu. V tomto prípade sa správy ukladajú v SMS centre a doručujú sa pri prvej ďalšej príležitosti. K dispozícii je často možnosť získať automatickú notifikáciu o doručení správy. Tieto a iné funkcie závisia od možnosti mobilného operátora.

3.4.1.2 DTMF (Dual Tone Multiple Frequency)

Zostavovanie hlasového spojenia patri medzi základné schopnosti mobilných sietí. DTMF – tónová voľba ponuka prenos dát po takto zostavenom hlasovom spojení. Jedná sa o prenos na princípe prepojenia okruhu. Jednotlivé DTMF tóny sa skladajú z dvoch amplitúdovo zložených sínusových signálov. V hlasovom kanále je vždy možné preniesť iba jeden tón, doba prenosu tónu je minimálne 50ms a po každom tone musí nasledovať minimálne 50 ms „ticha“. Z toho nám výjde prenosová rýchlosť 5 byte/s. Generovanie tónu je jednoduché, detekcia tónu je ale zložitejšia. DTMF sa v dnešnej dobe najviac využíva pre telefónnu voľbu a v rádiotechnike.

3.4.2 GPRS (General Packet Radio Service)

GPRS je paketovo orientovaný prenos dát v sieti GSM. Pre zvýšenie rýchlosti združuje jednotlivé hlasové kanály a je možné jedinému užívateľovi rezervovať všetkých osem kanálov jedného TDMA rámca. Rýchlosť závisí od spôsobu kódovania, ktoré sa volí samo zo štyroch dostupných možností podľa sily signálu GSM a vzdialenosti od vysielača. Rýchlosť ďalej závisí od počtu využitých kanálov. Pre IP komunikáciu je tu k dispozícii maximálna rýchlosť 160 kbit/s, skutočná rýchlosť sa tak pohybuje medzi 22-40 kbit/s. Štandardne sa pri prenose využíva 5 kanálov, väčšinou v konfigurácii 4+1 (4 pre download a 1 pre upload). Prenos má pomerne veľké oneskorenie okolo 500ms.

3.4.3 EDGE (Enhanced Data rate for GSM Evolution)

EDGE je v podstate to isté ako GPRS. Hlavný rozdiel je iba v použitej modulácii. EDGE používa moduláciu 8-PSK, ktorá dokáže preniesť 3 informačné bity pomocou jedného symbolu na rádiovej vrstve, na rozdiel od GPRS, kde je použitá modulácia GMSK, ktorá dokáže preniesť iba jeden informačný bit na jeden informačný symbol. Pri ideálnych podmienkach a použití všetkých osem kanálov je možné dosiahnuť rýchlosť 473.6 kbit/s. Skutočná rýchlosť sa pohybuje okolo 200 kbit/s pre download a 100 kbit/s pre upload, pri konfigurácii kanálov 3+2.

3.4.4 IS-95 A,B (Interim Standard – 95)

IS-95 pracuje na báze CDMA ktorá je najrozšírenejšia v Spojených Štátoch a vyvinutá firmou Qualcom. Na označenie tohto štandardu sa používa aj výraz CdmaOne a patrí do druhej resp. 2,5 generácie pri IS-95B.

Hlavný rozdiel medzi verziou A a B spočíva v rýchlosti spojenia na základe prepínania okruhov, a to 14,4kbit/s pri verzii A a 64kbit/s pri verzii B.

Na rozdiel od GSM a princípov TDMA a FDMA si technológia CDMA kóduje dáta špeciálnym kódom (napr. Walshov kód), ktorý je priradený ku každému kanálu. Pracovné frekvenčné pásmo je u tohto systému nastavené na 450MHz.

3.4.5 CDMA 2000 (Code Division Multiple Access)

CDMA 2000 využíva relatívne široké kanály (1.25 Mhz). Užívateľský signál je kódovaný jedným z unikátnych kódov, ktoré rozprestrú signál po celej šírke spektra prenosového kanálu. Vďaka tomu je možné, že na jednom kanále a v jednom okamihu komunikuje viacej užívateľov naraz.

Technológia CDMA 2000 zahŕňa štandardy CDMA 2000 1xRTT (1 x Radio Transmission Technology), 1xEV-DO (1 x Evolution Data Optimized) a CDMA 2000 1 x EV-DV (1 x Evolution Data/Voice)

Štandard 1xRTT je starší a poskytuje dvojnásobnú kapacitu na prenos hlasu a pre dáta poskytuje maximálnu rýchlosť 614 kbit/s. Štandard EV-DO je orientovaný na dátové prenosy čiže hovor tu ide uskutočniť najviac pomocou VoIP. Prenosové maximum je 2.4 Mbit/s pri modulácii 16-QAM a ideálnych podmienkach a 500 – 700 kbit/s s oneskorením okolo 200 ms. Tretí štandard EV-DV ponúka maximálnu rýchlosť 3.1 Mbit/s pre download a 1.8 Mbit/s pre upload. Zároveň podporuje súčasne aj dátové aj hlasové služby.

K dispozícii je aj modifikácia CDMA 450, ktorá je založená na CDMA EV-DO a umožňuje využitie tejto technológie v pásme 450 MHz.

3.4.6 UMTS (Universal Mobile Telecommunication System)

Sieť UMTS je považovaná za nasledovníka GSM a nesie označenie siete tretej generácie (3G).

K mnohonásobnému prístupu používa technológiou W-CDMA, ale taktiež kombináciu GSM princípov TDMA a FDMA.

Metóda W-CDMA (Wideband Code Division Multiple Access) je rozčlenená do kanálov o šírke 5 MHz, ktorá buď používa na prenos frekvenčný duplex (FDD) a je označovaná ako UMTS FDD. Ďalšou variantou je metóda TD-CDMA (Time Division CDMA), ktorá používa časový duplex.

Najviac využívané frekvenčné spektrum sa skladá z jedného párového pásma (1920 – 1980MHz ; 2110 – 2170Mhz) a jedného nepárového pásma (1910 – 1920MHz; 2010 – 2025Mhz). V roku 2000 boli pridelené ešte ďalšie 3 pásma, ale v Európe je použiteľné len jedno z nich, a to 2500 – 2690 MHz.

Dnes najčastejšie používané UMTS existuje vo viacerých verziách. Staršia verzia R99 dosahuje v praxi rýchlosti od 50 do 120 kbit/s. Novšia verzia R4 alebo podľa využívajúcej technológie HSDPA (High Speed Dowlink Packet Access) umožňuje rýchlosti až do 14,4Mbit/s. Verzia s úpravou rádiového rozhrania HSUPA zasa rieši nedostatok rýchlosti pre upload a to do rýchlosti až 5,76Mbit/s.Verzia R6 tiež prináša menšie oneskorenie pri prenose a to z pôvodných 100 až 200 ms na 50ms.

Plánované verzie R7 a R8 by mali v nasledujúcich rokoch ponúknuť mnohonásobne vyššie rýchlosti prenosu dát, ale momentálne sú tieto štandardy v štádiu vývoja a testovania.

- R3 (označovaný ako R99)
- R4 (označovaný ako R2000)
- R5 - HSDPA downlik (14.4 Nbps)
- R6 - HSUPA uplink (5.76 Mbps)
- R7 - HSDPA 28.8/HSUPA 11.5
- R8 - LTE (Long Term Evolution), HSPA evolution

4 OTÁZKY BEZPEČNOSTI

4.1 Bezpečnosť bezdrôtovej siete

Zaistenie bezpečnosti patrí medzi najťažšie úlohy bezdrôtovej komunikácie, pretože signál šíriaci sa vzduchom je mimoriadne ľahké zachytiť. Nejde len o zabezpečenie bezdrôtovej komunikácie na fyzických, či spojových vrstvách, ale aj o zabezpečenie na všetkých vrstvách sieťovej architektúry. Žiadne vyvinuté bezpečnostné riešenia v sieti nemôžu byt stopercentné. Ani silné normy a šifry nezaručujú, že systém odolá všetkým budúcim útokom. Vždy bude na koncovom užívateľovi, aby sa oboznámil s bezpečnostnými mechanizmami a porovnal ich so svojimi potrebami.

Problematika bezpečnosti je veľmi rozsiahla. Pozornosť preto venujem iba zabezpečeniu WLAN sieťam, ktoré budú tvoriť základ pre návrh riešenia komplexu budov (viď.kapitola *5*).

Bezpečnosť bezdrôtových sietí môžeme rozdeliť do dvoch hlavných skupín :

- **Šifrovanie** (zabezpečenie prenášaných dát pred odpočúvaním)
- **Autentizácia** (riadenie prístupu oprávnených používateľov)

Autentizácia v 802.11 je jednosmerný proces. Stanica musí o autentizáciu do siete zažiadať, zatiaľ čo sieť sa voči staniciam autentizovať nemusí.

802.11 špecifikuje 2 metódy autentizácie:

- Open-system autentizácia
- Shared-key autentizácia

V súčastnosti existujú 3 druhy protokolov, ktoré zabezpečujú ochranu WiFi sietí:

4.1.1 WEP

Skratka WEP (Wireless Equivalent Policy) je štandardom, ktorý definuje schému ochrany

bezdrôtových sietí 802.11 na úrovni druhej vrstvy OSI modelu.

Zabezpčuje komunikáciu medzi zariadeniami až na úroveň prístupového bodu. Za ním už bezpečnosť nezaistí. Štandard WEP používa simetrickú streamovú šifru RC4, teda šifru s tajným kľúčom. Odosielaná správa sa šifruje podľa nejakého kľúča (obvykle slova alebo sekvencie znakov) a na cieľovom bode sa zasa podľa tohto kľúča dešifruje. Prebieha to tak, že kľúč expanduje na pseudonáhodný kľúčovací tok (keystream) v rovnakej dĺžke akú má šifrovaná správa. O pseudonáhodnosť sa stará generátor pseudonáhodných čísel PRNG. Šifrovanie prebieha tak, že na šifrovanej hodnote sa vykoná logická operácia XOR s kľúčovacím tokom, dešifrovanie prebieha rovnako.

V súčastnosti existujú rôzne dĺžky šifrovacieho kľúča. Výrobcovia udávajú dĺžky 64,128 a 256 bitov. V skutočnosti je to trochu inak. Šifrovací WEP kľúč má dĺžku 40 bitov. Pred týchto 40 bitov sa predsadí 24 bitov inicializačného vektora. Tak isto je to pri dĺžkach 128 a 256 bitov. 24 bitov je vždy vyhradených pre inicializačný vektor.

4.1.2 802.1x

Je protokol umožnujúci autentizáciu na portoch (porty chápeme ako súčasť prvej sieťovej vrstvy, teda fyzické porty na prepínači).

802.1x blokuje všetku komunikáciu na danom porte až do doby, kým sa klient autentizuje prostredníctvom údajov, ktoré sú uložené na back-end servery. Základ 802.1x tvorí PPP protokol (Point to Point Protokol). PPP je obmedzený tým, že umožňuje autentizáciu založenú len na kombinácií užívateľského mena a hesla. Do budúcnosti sa počíta s protokolom EAP (Extensible Authentication Protokol), ktorý je rozšírením protokolu PPP. V EAP sa dajú používať heslá, certifikáty, tokeny, čipové karty, biometriká, atď. Počíta sa tu aj s možnosťou použiť mechanizmy, ktoré v súčasnosti ešte nie sú známe. Overenie v bezdrôtovej sieti zabezpečuje prístupový bod pomocou zoznamu, alebo externého autentizačného systému založeného na servery Kerberos.

4.1.3 802.11i

Tento štandard je platný pre všetky bezdrôtové siete a zakladá na šifrovaní pomocou šifry AES v rámci autentizačného rámca EAP. Implementácia AES si vyžiada zvýšenie výkonu

hardwaru pre šifrovanie a dešifrovanie.

Podmnožinou 802.11i je WPA, ktoré slúži na dočasné riešenie pre zvýšenie bezpečnosti. V čase nasadenia WPA ešte nebola hotová primárna časť protokolu 802.11i, ktorou je šifra AES.

Rovnako ako RC4, aj šifra AES je symetrickým kľúčom. AES pracuje s blokmi vo veľkosti 128 bitov a preto je označená ako bloková. Vystupuje tu i nový algoritmus MIC, ktorý zaisťuje aby nedošlo k modifikácií prenášaných dát. MIC je založený na inicializačných hodnotách.

Čítačkový režim šifrovania šifrou AES sa výrazne odlišuje od WEP a RC4. Výstupom šifry AES je po inicializácií len 128 bitový blok . Celý výstupný text sa rozdelí na 128 bitové bloky a tie sa postupne XORuju so 128 bitovým, vždy nanovo generovaným výstupom AES tak dlho, pokiaľ nedôjde k zašifrovaniu celej pôvodnej správy. Nakoniec sa čítač vynuluje. Výsledkom je oveľa silnejšia šifra.

4.1.4 RADIUS

Radius je AAA protokol (authentication, authorization and accounting) používaný pre prístup k sieti alebo pre IP mobilitu. Môže pracovať lokálne tak aj v roamingu. Pri pripojení k poskytovateľovi internetu pomocou vytáčaného pripojenia, DSL, alebo Wi-Fi je u niektorých poskytovateľov vyžadovane prihlasovacie užívateľské meno a heslo. Táto informácia je poslaná do takzvaného Network Access Server (NAS) zariadenia cez Point-to-Point Protocol (PPP). Potom je odovzdaná RADIUS serveru cez RADIUS protokol. RADIUS server overí pravosť informácii uplatnením autentizačných schém ako PAP, CHAP alebo EAP. Ak je užívateľské meno a heslo prijaté, server autorizuje prístup k poskytovateľovi Internetu a vyberie IP adresu (prípadne rozsah adries) a ďalšie parametre spojenia. RADIUS protokol neposiela hesla medzi NAS a RADIUS serverom v čistom texte (ani pri použití s PAP protokolom), používa sa MD5.

RADIUS bol pôvodne vyvinutý spoločnosťou Livingston Enterprises pre ich PortMaster série Network Access Servers a neskôr (1997) uverejnené ako RFC 2058 a RFC 2059 (súčasné verzie sú RFC 2865 a RFC 2866). Momentalne existuje niekoľko komerčných open-source RADIUS serverov ktoré sa líšia najme vlastnosťami.

4.1.5 Wireless LAN Solution

Vo veľkých počítačových sieťach je možný vznik ďalších rizík. Jedným z rizík je tá skutočnosť ,že zamestnanci môžu priniesť svoj AP a ten napojiť na existujúcu metalickú sieť tým môžu vzniknúť neoficiálne prístupové body. Z pohľadu administrátora siete a zodpovednej osoby za bezpečnosť siete, môžeme využiť aj ďalšie nástroje, ktoré môžu odhaliť tieto "nelegálne" prístupové body. Jedným z takýchto riešení je produkt spoločnosti Cisco - CiscoWorks Wireless LAN Solution Engine (WLSE). Na základe komunikácie medzi týmto zariadením a prístupovými bodmi možno zistiť dostupnosť ďalších sietí v dosahu access pointov + lokalizácia.

4.2 Bezpečnosť objektu podniku

Pri identifikácii bezpečnostných rizík daného podniku vychádzam z reálnych kritérií, ktoré sú v danom objekte vopred nastavene a značnou mierou sa podieľajú na eliminácii hrozieb, ktoré na firmu môžu pôsobiť.

Hlavným predpokladom realizácie systému komplexnej bezpečnosti organizácie na elimináciu bezpečnostných rizík, je správny vyber vhodných technických, personálnych, organizačných a technologických riešení a určenie povinnosti z nich vyplývajúcich pre manažment a zamestnancov v rozsahu svojej pôsobnosti.

4.2.1 Vonkajšia technická a fyzická ochrana

Stav vonkajšej bezpečnosti je riešený zmluvne fyzickou ochranou objektu organizácie súkromnú - bezpečnostnú službu, kde v rámci objektu sú príslušníci ochrany objektu SBS v určenom priestore pri hlavnom vchode do objektu organizácie, kde kontrolujú vstup a výstup zamestnancov ako aj dodávateľov. Pohyb osôb sa permanentne reguluje tak aby nedošlo k nekontrolovateľnému pohybu nepovolaných osôb do záujmových priestorov.

Okolie objektu je z pohľadu pasívnej bezpečnosti zabezpečené ochranným oplotením s nehybnými a tuhými pravidelnými ockami. Oplotenie je vo výmere 630m a s nadstavbami s ostnatým drôtom dosahuje výšku 2,8m. Odolnosť plota sa v prípade potenciálneho narušiteľa zvyšuje prvkami aktívnej bezpečnosti.

4.2.2 Prvky aktívnej bezpečnosti.

Monitoring chráneného vnútorného priestoru je zabezpečený pomocou kamerového systému značky Avigilon so záznamom a vyhodnocovaním daných strategických priestorov ale aj v okolí priľahlých oploteniu, ktoré sa nachádzajú v tesnej blízkosti. Tento kamerový systém je pripojený k LAN sieti podniku a prostredníctvom tejto siete sa pripája na vzdialenú správu pre oprávnených používateľov pultu centrálnej ochrany. V objekte sa nachádza 12 kamier s vhodne umiestnenými metahalogenovymi reflektormi aktivovanými pri narušení objektu, čo výrazne zjednodušuje činnosť zásahových skupín SBS a spôsobuje tak odstrašujúci faktor pre potenciálneho narušiteľa.

Obr.11 Kamerový zabezpečovací systém

Zdroj: ***www.avigilon.com***/

Riadenie kontroly vstupu osôb do areálu ako aj vo vnútorných priestorov je zabezpečené prostredníctvom elektronických zámkov a vstupným turniketom v systéme prístupových a komunikačných jednotiek. Tento systém je prepojený v rámci celého objektu a zabezpečujú ho riešenia firmy RYS a jeho serverovej aplikácie s názvom BBIQ. Na základe individuálne nastavených oprávnení je riadený vstup oprávnených osôb po celom objekte.

Kontrola vstupu pre vozidla je taktiež riadená v kombinácii z prístupovým aj kamerovým systémom a využíva sa posuvná brána na koľajnici s elektronickým pohonom a ovládaním.

4.2.3 Vnútorná ochrana objektu

Na základe individuálne nastavených oprávnení je riadený vstup oprávnených osôb po celom objekte. Elektronické čítacie zariadenia a zámky sú navrhnute pre rovnaký systém firmy RYS ako aj turniket a vstupná elektronická brána. Využívajú sa bezkontaktne čipové prívesky, ktoré sú okrem prístupových systémov využívané aj na riadenie dochádzky a taktiež dokážu spolupracovať so systémom stravovania.

Vybrané priestory objektu sú zabezpečené poplašnou signalizáciu narušenia, ktoré dokážu zachytiť možný potenciálny prienik do chráneného objektu ešte skôr ako by sa tam narušiteľ mohol dostať. Včasná signalizácia umožňuje adekvátne zareagovať (poplach a, upozornenie strážnej služby SBS) a tým zabrániť poškodeniu vonkajšieho plášťa a chránených objektov pred prípadným rozbitím okna, vypáčením dverí, poškodením múrov a pod. Toto elektronické zabezpečenie vybraných objektov s poplašnou signalizáciou pri ich narušení zahŕňa poplachovú ústredňu, pohybové snímače, GSM hlásiče, sirény, prístupové klávesnice a moduly na komunikáciu s PC. Systém je flexibilný a je ho možné jednoducho rozšíriť v prípade ďalších požiadaviek na tento typ zabezpečenia.

Podmienky na ochranu života a zdravia osôb, majetku a životného prostredia pred požiarmi sú dodržiavané určené a presne stanovene kritéria (zákon c.314/2001 Z.z).
V priestoroch organizácie sa nachádza elektronická požiarna signalizácia EPS, ktorá dokáže včasne detekovať možný vznikajúci požiar a vykonať následné vyhlásenie poplachu. EPS poskytuje okamžité informácie o požiari, ktoré dokáže odosielať na pult centrálnej ochrany.

Obr.12 Elektronicka poziarna signalizacia

Zdroj: ***www.minimax.de/***

II PRAKTICKÁ ČASŤ

5 NÁVRH RIEŠENIA BEZDRÔTOVEJ SIETE

Pre môj alternatívny návrh som si zvolil štandard 802.11n (2.3.6 Štandard 802.11n), nakoľko poskytuje prijateľné riešenie pre poskytovanie bezdrôtovej komunikácie. Postačujúco nám dokáže pokryť celý objekt a taktiež zabezpečiť veľmi dobrú bezpečnosť, nie veľmi náročnú správu a prijateľnú cenu nákladov v porovnaní s inými typmi sietí. Nebudem robiť kompletný návrh, pretože v danom komplexe budov už funguje stabilná pevná sieť, ktorú opíšem v kapitole *5.1*. Pokúsim sa navrhnúť alternatívu infraštruktúry k tejto sieti, ktorá môže poskytnúť zamestnancom tejto firmy väčšiu flexibilitu. (kapitola *5.2*)

Pre lepšie predstavenie si objektu prikladám satelitnú snímku vid Obr. 11, a taktiež popis jednotlivých častí celého komplexu viď **Obr. 13**. Umiestnenie firmy je v neobývanej časti mesta a najbližšie obývaná časť je vzdialená 2km, čo je veľkým pozitívom z hľadiska bezpečnosti a konkrétne neželaného odpočúvania.

1. Administratívna budova
2. Technický blok
3. Jedáleň
4. Sklad 1
5. Sklad 2
6. Vrátnica

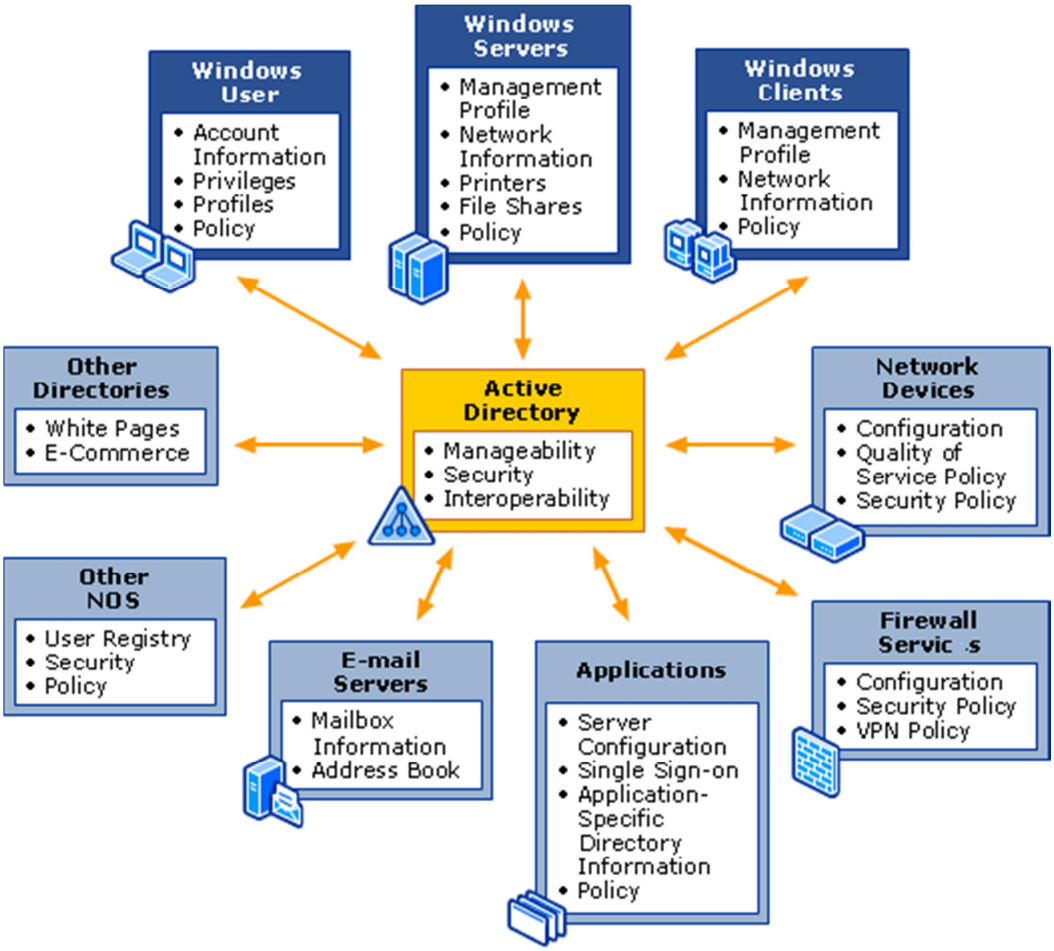
Obr.13 Satelitná snímka objeku

Zdroj: ***www.maps.google.com***

5.1 Popis súčasného stavu fixnej LAN siete

Táto sieť je typu klient – server, kde server plní funkciu poskytovateľa všetkých služieb pre klienta. Navrhnutá je ako sieť s doménou, kde server plní funkciu radiča domény (Active directory), a to z dôvodu vyššieho počtu počítačov a pripojených používateľov. Táto skutočnosť zabezpečuje fungovanie centrálnej správy a monitorovania. AD ukladá informácie o užívateľoch, počítačoch a sieťových zdrojoch a sprístupňuje tieto zdroje

užívateľom a aplikáciám. Poskytuje jednotný spôsob pre pomenovanie, popis, lokalizáciu, prístup, správu a zabezpečenie týchto zdrojov. Ďalšie informácie o AD sú dostupné na stránke: ***http://www.ervin.sk*** . Pospis funkcií radiča domény je stručne znázornený na **Obr.14**



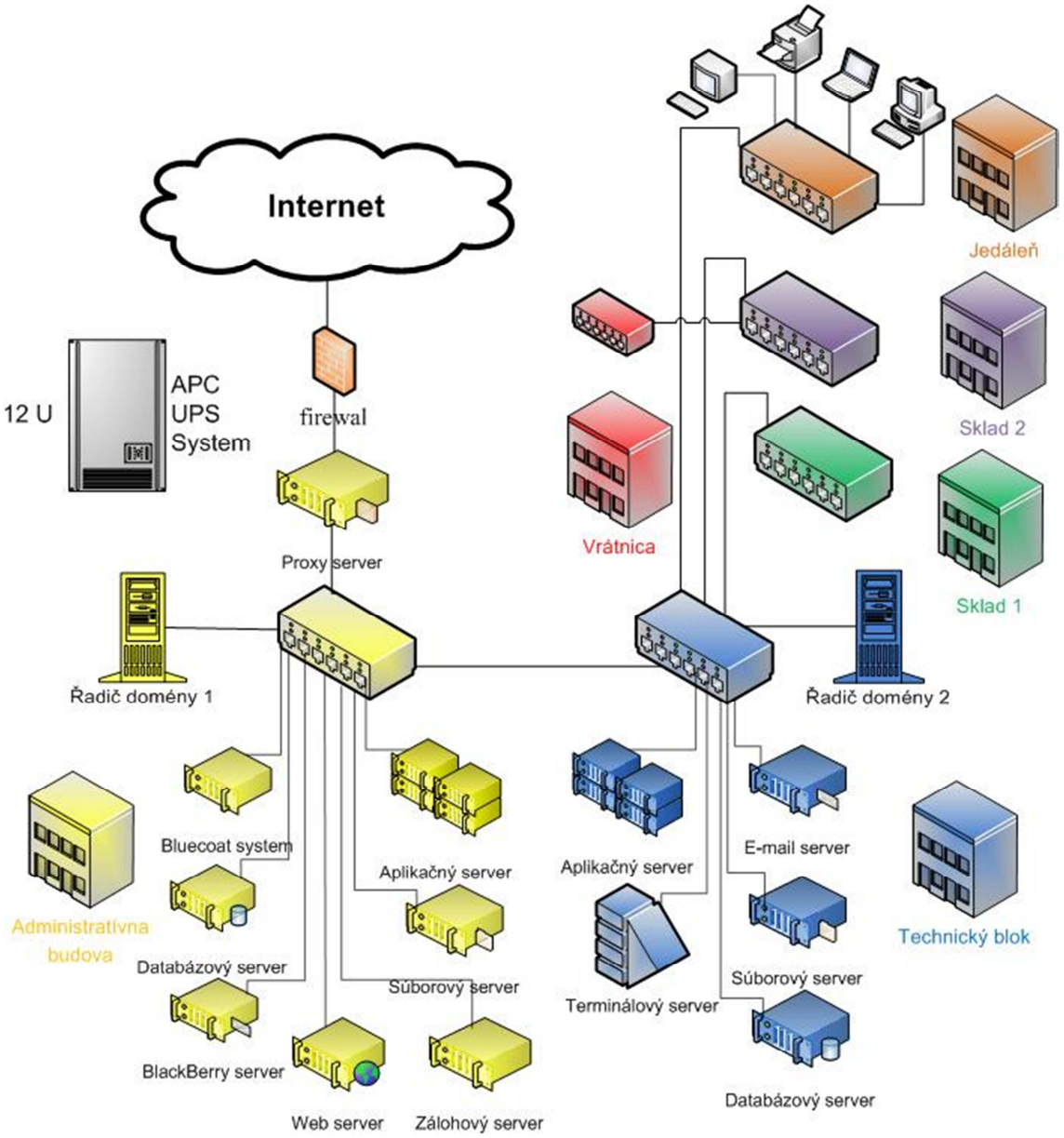
Obr.14 Popis funkcií radiča domény (AD)

Zdroj: ***www.wasolutions.ne***t

Sieť ďalej disponuje aj zdieľaným diskovým priestorom pre výmenu a uchovávanie dát (4.1.7) ale aj možnosťou zálohovania dôležitých dát (4.1.8). Celková štruktúra je navrhnutá nielen vzhľadom k súčasným požiadavkám firmy, ale aj vzhľadom k budúcemu možnému rozširovaniu siete, pridávaniu počítačov, alebo zvýšeniu počtu používateľov. Ziednodušené zobrazenie architektúry tejto siete spolu s prehľadom hardwarových zariadení a jednoduchým popisom je zobrazené na **Obr.15**.

5.1.1 Serverová základňa

V objekte budov sú umiestnené dve serverovne. Jedna z nich je v priestoroch administratívnej budovy a tá druhá v technickom bloku. Tu sa nachádzajú všetky dôležité komponenty a zariadenia siete. Ostatné budovy a všetky poschodia majú vlastnú RACK room. Zjednodušený model súčasného stavu fixnej siete v danej firme a jej komplexe jednotlivých budov viď **Obr. 15.**



Obr. 15 – Model architektúry súčasného stavu siete

Serverová základňa pozostáva zo serverov značky Fujitsu Siemens. Použitý typ RX 200 poskytuje moderné integrované štandardy, ako sú funkcie modular RAID, 4 hot-plug SAS disky, mirrorovaná pamäť. Vďaka vynikajúcej výkonnosti dvoj- a štvorjadrových procesorov intel Xeon, s rýchlejším FSB a väčšou L2 cache pamäťou dosahuje vysokú celkovú produktivitu. Zdroj ***www.fujitsu.siemens.com***

Ako operačný systém serverov je využitý Windows 2008 R2 Enterprise Server, vzhľadom k jeho širokým možnostiam nasadenia, nastavenia zabezpečení pre jednotlivých používateľov, jednoduchej vzdialenej správe a vysokej stabilite prostredia.

Celá sieťová infraštruktúra je prepájaná pomocou inteligentných prepínačov cisco catalyst 2960G,ktore sú určené pre siete fast a gigabitethernet. Tieto prepínače obsahujú integrované bezpečnostné funkcie ako ACLs (access control list) a DHCP Snoping. Taktiež tu je rozšírená podpora pre administrátorskú kontrolu a funkcie pre zistenie kvality služieb QoS. Použité sú 3 prevedenia tohto prepínača s 8, 24 a 48 portov.

Medzi routrom a sieťou, ktorú ochraňuje je zapojený hardwarový firewall a proxy server, ktorý komplexne zabezpečuje ochranu proti útokom zvonku. Vnútorné pripojenie do internetu zasa ochraňuje Bluecoat proxiSG ktorý, zvyšuje efektivitu využitia internetovej konektivity a súčasne pracovnej doby zamestnancov.

5.1.2 Funkcie serverov

5.1.2.1 E-mailovy server

Na spracovanie e-mailových správ a účtov slúži Microsoft exchange server. Umožňuje definovať používateľov, ktorým má byť triedená pošta z doménového koša doručená. Taktiež umožňuje definovať pravidlá pre triedenie pošty a jej automatické sťahovanie zo servera. Používatelia majú k svojej pošte prístup pomocou protokolov POP3, IMAP. Samozrejmosťou je SMTP server, slúžiaci na odosielanie pošty. E-mailový server je nastavený tak, aby mali používatelia možnosť internej komunikácie v rámci firmy, ale aj verejnej komunikácie .

5.1.2.2 Tlačový server

Tlačový server sa používa na poskytnutie prístupu k jednej alebo viacerým sieťovým tlačiarňam. V podniku sa nachádza 35 sieťových tlačiarní, od malých používaných na občasné pomalé tlačenie, až po veľké multifunkčné zariadenia s veľkou kapacitou tlače a množstvom iných doplnkových funkcií.

5.1.2.3 Súborový server:

V súborovom serveri sa centrálne nachádzajú všetky dokumenty, čím máme vytvorený určitý typ knižnice dokumentov. Keď používatelia vyžadujú súbor, spravidla si vyhradia celý súbor zo súborového servera, pracujú na ňom lokálne na svojej pracovnej ploche a potom ho vrátia späť.

5.1.2.4 Aplikačný server:

Tento server nám podobne ako súborový server slúži ako skladisko informácií. Sú v ňom uložené databázy SQL. Avšak na rozdiel od súborového servera, aplikačný server spracúva informácie tak, aby dodával len konkrétne údaje, ktoré používateľ, resp. klient vyžaduje.

5.1.2.5 WEB server

Slúži na umiestnenie internetovej stránky firmy. Táto internetová stránka sa nazýva intranet. Tu môžu pracovníci tiež zdieľať informácie pomocou tejto internej webovej lokality. Na tejto lokalite sa vytvárajú knižnice zdieľaných dokumentov a tak isto sa zverejňujú oznamy, udalosti a dôležité informácie.

5.1.2.6 Zálohový server

Na tomto serveri je aplikovaný Weritas Backup Exec od spoločnosti Symantec. Tento software umožňuje úplne automatizovaný spôsob zálohovania dát bez spustenia, či intervencie používateľa. Je možné zadefinovať čas, kedy sa budú vybrané dáta zálohovať, ako aj typ záloh – úplný či prírastkový. Je možné uchovať niekoľko spätných verzií zálohovaných dát.

5.1.2.7 BlackBerry server

BlackBerry Enterprise Server for Microsoft Exchange umožňuje synchronizovať firemné emailové účty, kalendár, kontakty, poznámky a úlohy s mobilnými BlackBerry zariadeniami. Znamená to asi toľko, že každý nový email, každá zmena v úlohách, poznámkach alebo kontaktoch sa automaticky prenesie aj do mobilného BB zariadenia daného človeka. A rovnako aj opačne.

5.1.3 Pripojenie k sieti internet

Pripojenie k sieti internet je zabezpečené prostredníctvom digitálnej telefónnej linky, poskytujúce nielen hlasové služby pre firmu, ale aj vysokorýchlostný internet. Pripojenie je typu ADSL a jeho rýchlosť je 512 kbit/s. Vzhľadom k počtu pripojených počítačov do siete LAN je táto rýchlosť s rezervou postačujúca. Keďže server bude nakonfigurovaný pre prístup PROXY, bude disponovať vyrovnávacou pamäťou pre zníženie záťaže internetu pri často navštevovaných stránkach. Internetový prívod je priamo zo vstupného bodu privedený cez ADSL modem alebo router na jeden zo sieťových adaptérov servera. Na druhý je pripojená lokálna sieť LAN.

5.1.4 Zabezpečenie neprerušenej prevádzky systému

Servery, prepínače a ostatné dôležité komponenty serverovej ústredne sú ku zdroju napájania pripojené cez UPS zariadenia (Uninterruptable Power Source – neprerušiteľný zdroj napájania), ktoré zabezpečujú prevádzku serverov po dobu 10 až 15 minút po výpadku elektrickej energie, čo predstavuje postačujúcu dobu na nábeh diselových agregátov, ktoré vyrábajú elektrickú energiu, a tým zabezpečujú neprerušenú prevádzku. Použitých je viac UPS zariadení značky APC s kapacitou od 3000VA až do 10000VA.

5.1.5 Počítačové vybavenie

Keďže primárnym použitím počítačov je kancelárska činnosť, ich hardwarové vybavenie by malo zodpovedať týmto požiadavkám. Pre kancelársku činnosť sú postačujúce počítače s procesorom Intel Celeron 1,7 GHz, 512MB RAM a 80GB diskového priestoru. Vhodná je mechanika CD-RW alebo DVD/CDRW Combo. Monitory 17” LCD, spolu so správnou

klávesnicou a myšou vytvárajú vhodnú ergonómiu prostredia. Ako operačný systém je najvhodnejší Microsoft Windows 7 – eterprise edition, vzhľadom k jeho použitiu a cene licencií. Kancelársky balík je navrhovaný Microsoft Office 2010 Proffesional. Ako antivírusový systém pre tieto počítače je najvhodnejší NOD32 od spoločnosti ESET

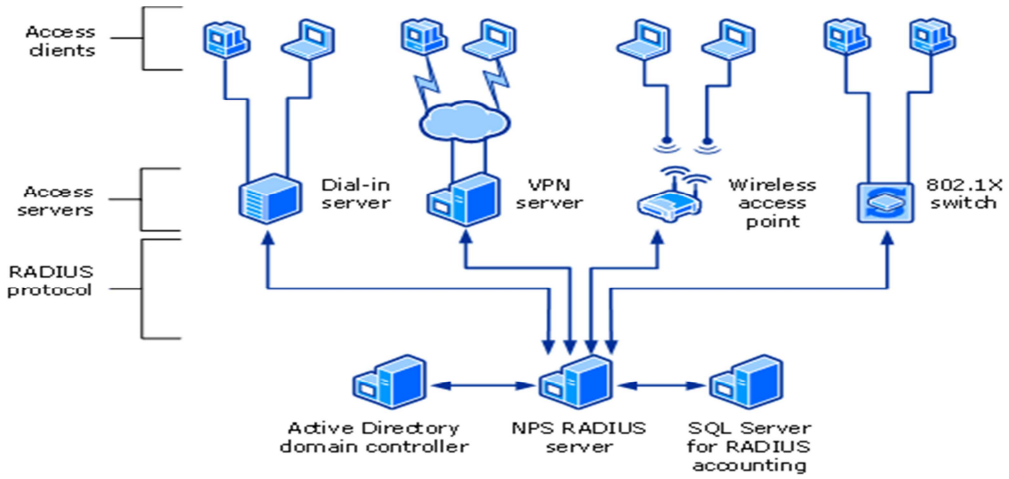
5.2 Implementácia bezdrôtovej siete

5.2.1 Architektúra

Ako už bolo spomenuté v úvode odseku *5. - Návrh riešenia bezdrôtovej siete*, pokúsim sa navrhnúť a popísať architektúru alternatívnej infraštruktúry k už fungujúcej stabilnej pevnej sieti popísanej v kapitole *5.1*.

Pre každú anténu je potrebný jeden Access point. V jednotlivých prístupových bodoch sú umiestnené riaditeľné prepínače podporujúce L2/L3 switching, v ktorých sú napojené jednotlivé access pointy. Tieto prepínače sú ďalej napojené do serverovne a konkrétne do centrálneho prepínača a aplikačného servera, kde sa do databázy zaznamenávajú všetky informácie. Pre lepšie pochopenie viď Obr. 17.

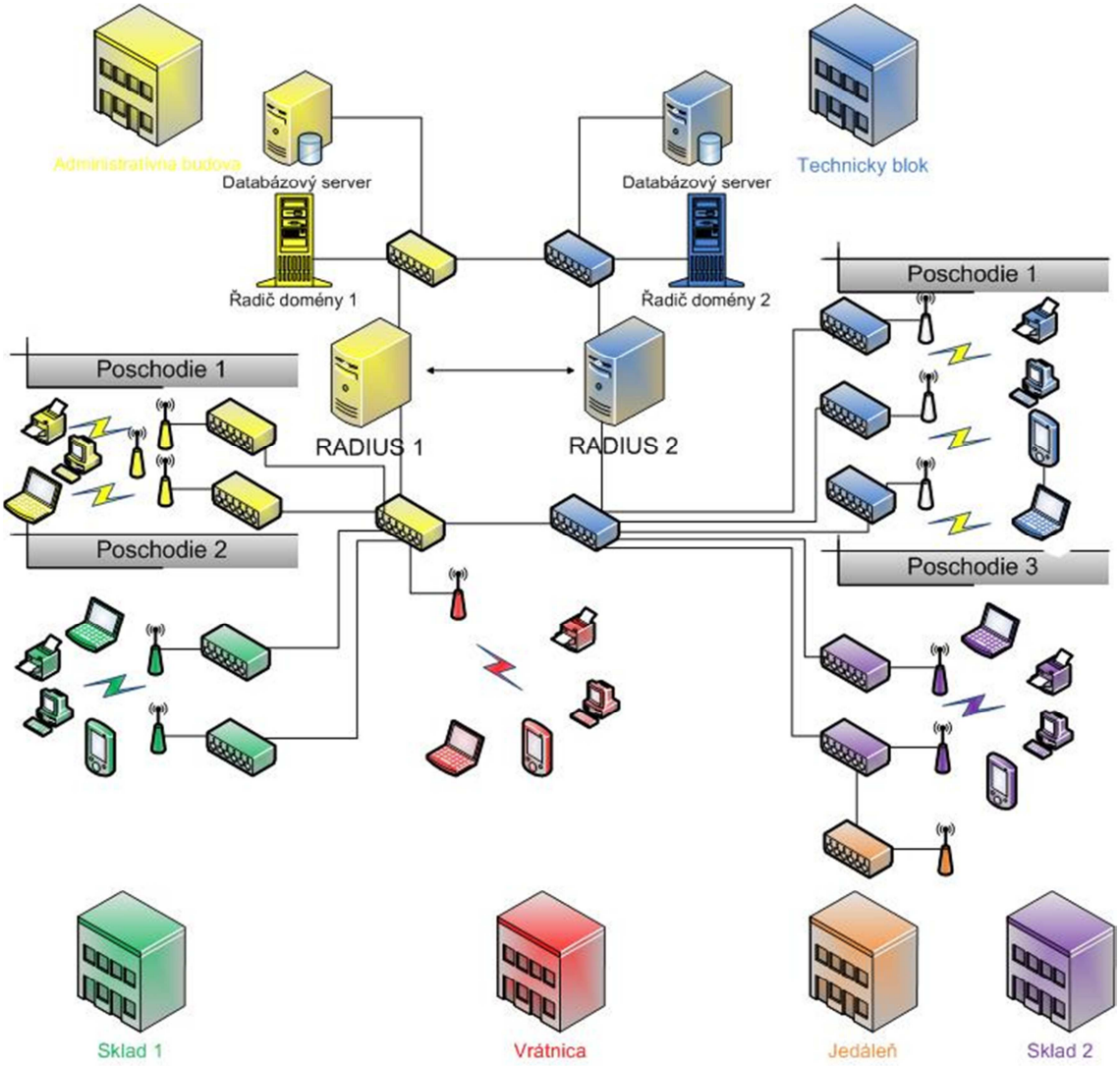
Na tomto mieste treba pôvodnú sieť doplniť o dôležitý prostriedok na autorizovanie klientov a je ním RADIUS sever viď (4.0), ktorý slúži na riadenie prístupu autorizovaných klientov do siete a zaisťuje distribúciu zdieľaných kľúčov pre šifrovanie komunikácie. Pre lepšie pochopenie ako začleniť radius server do siete pripájam **Obr. 16**.



Obr.16 Rádius server v bezdrôtovej sieti

Zdroj: *http://i.technet.microsoft.com*

Architektúra navrhovanej infraštruktúry je znázornená na **Obr.17**. Jednotlivé farby predstavujú, v ktorej budove je zariadenie umiestnené (vid *4.0*) Služba dial in a tiež VPN znázornené na **Obr.16** sa v mojom návrhu nevyskytujú, ale v prípade potreby by sa tieto služby dali bez problémov integrovať.



Obr.17 Architektúra navrhovanej infraštruktúry siete

5.2.2 Pokrytie

Dobré pokrytie nám dovolí, aby sa v akomkoľvek mieste objektu dalo bez problémov pripojiť a autorizovať do firemnej siete v rámci jednotlivých budov. Signál by mal byť nasmerovaný do využiteľných miest podľa koncentrácie používateľov. Prístupové body preto tvoria logickú štruktúru. Umiestnené sú podľa vzdialenosti, s prihliadnutím na okolie, ktoré môže brániť prechodu signálu, a tým znemožniť komunikáciu. Vzhľadom k počtu antén a použitých prístupových bodov je ale viac než pravdepodobné, že jednotlivé

kanály budú viacnásobne použité v rôznych oblastiach. Pokrytie by malo zabezpečiť celkovo 20 routerov s namontovanými vše smerovými anténami typu Cisco AIR-ANT2465 pre použitie v oblastiach s menšou koncentráciou prekážok. Naopak antény typu Cisco AIR-ANT2485P so ziskom 8.5 db by mali pokryť aj miesta ťažko dostupné prechodu signálu. Pokrytie sa ale nedá presne určiť bez testu v reálnej situácii.

5.2.3 Hardware

Pre návrh som si zvolil profesionálne hardwarové zariadenia značky Cisco IEEE AIR-AP1242N WLAN QoS, ktoré dokážu zdokonaliť kvalitu v aplikáciách pracujúcich so zvukom, obrazom ale aj prenosu hlasu po bezdrôtovej sieti. Toto AP minimalizuje čas odozvy a poskytuje optimálne využitie pre všetkých užívateľov. Podporuje všetky styri štandardy 802.11a,b,g,n .

Obr.18 Prístupový bod Cisco AIR-AP1242N

Zdroj:***www.cisco.com***

Tab.4 Hlavne funkcie prístupového bodu Cisco AIR-AP1242N	
Rozhranie	802.11a,b,g,n
Bezpečnosť	802.11i, 802.11x, WPA, WPA2, AES, TKIP

Pamäť	32 MB RAM 16 MB flash
Konektory	Duálne RP-TNC
Skladovacia teplota	-40 až 85 stupňov C
Pracovná teplota	-20 až 55 stupňov C
Pracovná vlhkosť	10 až 90 percent
Napájanie	Miestne napájanie, Cisco Aironet Injektory AIR-PWRINJ3
Rozmery	16,76 x 21,59 x 2.79 cm

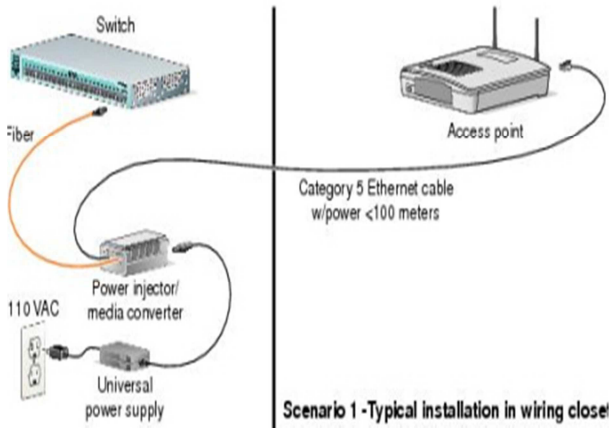
Tento prístupový bod je určený pre prácu vo vnútornom prostredí. Na osadenie do vonkajšieho prostredia, požijeme plne kompatibilný plastový box od firmy Cisco zobrazený na **Obr.19**

Obr.19 Plastový box Cisco Aironet 1522AG

Zdroj:***www.cisco.com***

Power injector Cisco AIR-PWRINJ3 (**Obr.21**) slúži ako PoE (*Power over Ethernet)* na napájanie prístupových bodov, pomocou sieťového káblu bez nutnosti pripojenia napätia k prístroju, pomocou ďalšieho samostatného káblu. Presne zapojenie je načrtnuté v **Obr.20**

Väčšina vzdialených prístupových bodov je umiestnená na miestach bez prístupu elektrickej energie. Použitie techniky PoE je veľkým prínosom a možnosťou ušetrenia nemalých prostriedkov na vybudovanie elektrickej siete ku každému prístupovému bodu.



Obr.20 Zapojenie power injectoru **Obr.21 Power injector Cisco AIR-PWRINJ3**

Zdroj:***www.cisco.com***

Prechod na bezdrôtovú sieť bude znamenať aj pre používateľov doplnenie hardverových komponentov, ako napríklad bezdrôtové karty alebo printservery na použitie tlačiarni v bezdrôtovom prostredí. Nie veľmi drahé profesionálne zariadenia s plnou podporou použitých prístupových bodov Cisco sú zariadenia ako Cisco Linksys WMP600N (**Obr.22**), Cisco Linksys WUSB600N (**Obr.23**) a Cisco Linksys WPS54G (**Obr.24**)

Obr.22 Cisco WMP600N **Obr.23 Cisco WUSB600N** **Obr.24 Cisco WPS54G**

Zdroj:***www.cisco.com***

Prenos signálu je úlohou použitých profesionálnych antén od spoločnosti Cisco, ktorých prehľad je uvedený v prílohe 1, 2 a 3.

5.3 Bezpečnosť

Ako bolo spomenuté v objekte budov sú umiestnené dve serverovne. Vstup do týchto miestností majú povolený len administrátori a top managemet v ich sprievode. Miestnosti sú uzamknuté a kľúče majú k dispozícii iba administrátori tohto systému.

Každá z nich má vlastný požiarny systém a spoločný IT monitoring miestnosti a infraštruktúry.

IT monitoring serverovne je informačný monitorovací systém elektronických zariadení, ktoré efektívne monitorujú prostredie a informácie o kritických hodnotách dokážu posielať v rámci siete a pomocou GSM jednotky na mobilne zariadenia správcom systému on-line. Hodnoty jednotlivých senzorov sa jednoducho dajú sledovať pomocou web rozhrania, kde sa všetky zaznali ukladajú do reportových súborov. Jednotlivé reporty tvoria zdroj informácii, ktoré sa pravidelne vyhodnocujú a poskytujú podklad na obnovu a inovácie zariadení. Dane serverovne monitorujú jednotky vyrábané spoločnosťou SEAL v typovej rade Poseidon, ktoré dokážu zabezpečovať nasledovne funkcie:

- Meranie teploty
- Meranie vlhkosť v miestnosti alebo v rozvádzači
- Detekcia zaplavenia alebo prítomnosť vody
- výpadok napájacieho prúdu
- prítomnosť dymu
- prítomnosť plynu a horľavých látok
- otvorenie dverí
- pohyb v miestnosti
- prietok vzduchu pri ventilátoroch
- meranie/kontrola napätia

Obr.25 IT monitoring system

Zdroj: ***www.seal.sk/***

Ďalšou dôležitou súčasťou výbavy serverovne sú výkonné klimatizácie, ktoré zabezpečujú permanentnú teplotu. V každej so serverovni sú redundantne klimatizačné jednotky, ktoré pracujú samostatne a tým je zaručená ich neprerušená prevádzka. V pravidelných termínoch je zabezpečovaná dôkladná údržba a starostlivosť o tieto veľmi dôležité komponenty.

5.3.1 Ochrana vnútorných citlivých informácii

Ochrana vnútorných citlivých informácii je veľmi dôležitá z hľadiska bezpečnosti údajov, ktoré okrem toho že sú dôkladné chránené, musia byt aj monitorovane aby sa zabránilo ich neoprávneným unikom a zneužitiu. Identifikácia a klasifikácia dôverných informácii, je v podniku spracovaná v smernici na ochranu citlivých dôverných a chránených dokumentov a informácii organizácie.

5.3.2 Antivírusová ochrana a ochrana proti útokom zvonku

Antivírusová ochrana je riešená pomocou programu Scan Office od spoločnosti Trend Micro, zabezpečuje kontrolu všetkých dát prechádzajúcich cez server, či už z internetu alebo cez e-mail. Chráni tak pred vírusovými infiltráciami nielen server samotný, ale aj používateľov pristupujúcich k internetu, alebo ku svojej pošte. Používatelia majú vytvorené vlastné používateľské kontá, ktoré im umožnujú prístup k zdieľanému diskovému priestoru, aplikáciám, dokumentom a internetu. Zároveň je možné pomocou

manažéra diskových kvót obmedziť využitie diskového priestoru, aby nedošlo k jeho zneužívaniu alebo neúmernému plytvaniu.

Ochrana proti útokom zvonku je zase riešená už spomínaným firewall systémom (*5.1.1*) a Bluecoat proxiSG zasa ochraňuje vnútorné pripojenie na internet, ako aj zvyšuje efektivitu využitia internetovej konektivity a pracovnej doby zamestnancov.

5.3.3 Napojenie na bezpečnostný systém

Výhodou z hľadiska bezpečnosti je poloha tohto komplexu budov. Nachádza sa približné 2 km od najbližšie obývanej oblasti. Týmto sa výrazné redukuje možnosť útoku, pretože antény umiestnené vo vnútri budov, by signál nemali šíriť ďalej ako 200metrov od areálu.

Umiestnenie prístupových bodov do uzamykateľných plastových boxov ma tiež bezpečnostný charakter. Nedovoľuje resp. sťažuje možnosť fyzického prístupu k prístupovým bodom z interného prostredia firmy

Okrem zabezpečení, ktoré boli spomenuté sa na bezpečnosti podieľa najviac Radius server, ktorého pripojenie do štruktúry je znázornené (vid. **Obr.19**) a okrem neho sú všetky v návrhu použite zariadenia s plnou podporou doplnkovej normy IEEE 802.1x

(vid kapitola *4*) .

Ostatné bezpečnostné prvky ako už spomenutý IT monitoring serverovne čí kontrola vstupu a kamerový systém sú do informačného systému pripojené pomocou pevných drôtových rozhraní privedených priamo na switche v serverovniach. Tu sú jednotlivé aplikácie nainštalované na aplikačných serveroch, ktoré tvoria cluster.

6 EKONOMICKÉ ZHODNOTENIE

Návrh bol pomerne konkrétny a tak nie je problém stanoviť náklady spojene s výstavbou tohto systému. Ceny sú získané z internetových obchodov ***www.swsd.sk*** pre produkty spoločnosti Cisco a ***www.edsystem.sk/*** pre ostatne potrebne komponenty. Na návrhu boli použite profesionálne zariadenia, ktorých cena je značne vyššia ako ceny lowend príslušenstva.

Tab.5 Prehľad cien a množstva zariadení potrebných na realizáciu návrhu

	Typ	**množstvo**	**Cena za kus**	**Celková cena**
Prístupový bod AP	Cisco AIR-AP1242N	20	499 €	9980 €
AP Directional anténa 8,5dBi	Cisco AIR-ANT2485P	4	160 €	640 €
AP Directional anténa 6dBi	Cisco AIR-ANT2465	16	145 €	2320 €
Power Injector	Cisco AIR-PWRINJ3	20	43 €	860 €
Switch 24 port	Cisco Catalyst 2960G 24	1	1270 €	1270 €
Switch 8 port	Cisco Catalyst 2960G 8	2	529 €	1058 €
WNIC (PC)	Cisco Linksys WMP600N	200	36 €	7200 €
WNIC (Laptop)	Cisco Linksys WUSB600N	30	36 €	1080 €
Wireless print server	Cisco Linksys WPS54G	40	47 €	1886 €
SPOLU	-	351	-	**30190 €**

Na každý jeden vysielač ďalej pripadá 65 € za konektory, káble, izoláciu, prepätovú ochranu atď. K týmto nákladom je nutné pripočítať náklady na samotné vybudovanie siete, predovšetkým so samotnou inštaláciou a konfiguráciou zariadení.

Odhadovaná celková cena tohto návrhu sa približuje sume **50000 €**

ZÁVER

V tejto práci sa mi naskytla možnosť spoznať a lepšie sa orientovať v množstve nových technológií, ktoré sa v relatívne krátkej dobe vyvinuli a dostali do našich bežných životov. Poskytuje prehľad z pohľadu bezpečnosti prenosových médií vo forme bezdrôtových sieti, ktoré predstavujú moderný trend v mobilnej hlasovej i dátovej komunikácií. Mobilita, flexibilita, prispôsobiteľnosť a úspora nákladov sú nezanedbateľné výhody týchto riešení. Okrem popisu technického riešenia a funkcii bezpečnostných prvkov som sa v tejto práci zaoberal množstvom ďalších otázok fungovania informačného systému ako takého. Načrtol som spôsob fungovania jednotlivých sieťových prvkov a ich komunikácie s prvkami zabezpečenia objektu a monitorovania. Pri riešení praktických otázok som sa inšpiroval systémovým prístupom organizácie, ktorá svojim spôsobom hľadá riešenia pri návrhu nových možnosti v inovatívnych informačných technológiách. V dnešnom dynamickom svete technológii je veľmi dôležité držať krok z inováciami a tiež treba sledovať zvyšujúci sa tlak na zabezpečenie systémov voči rôznym druhom útokov a rizík. Množstvo nových informácii pribúda každým dnom a spôsob udržania si prehľadu je aspoň z môjho pohľadu systémového administrátora veľmi dôležité.

V otázke bezpečnosti je informačný systém podniku ďaleko komplikovanejšou interdisciplinárnou záležitosťou. Cely systém bezpečnosti organizácie musí byt vytvorený tak, aby pomocou ľudských zdrojov, technických prostriedkov a organizačných opatrení zabezpečoval v dnešnej zložitej informačnej dobe spoľahlivú a efektívnu ochranu.

ZÁVER V ANGLIČTINE

In this work, I got an opportunity to learn and easier to navigate the many new technologies that are in relatively short time developed and given to our normal lives. It provides an overview in terms of security of transmission media in the form of wireless networks, which represent the modern trend in mobile voice and data communications. Mobility, flexibility, scalability and cost savings are not insignificant advantages of these solutions. In addition to the description of the technical solution and the function of safety features, I dealt with in this paper a number of other questions the functioning of the information system itself. I outlined the way the individual network elements and communication elements of the building and security monitoring. In addressing the practical issues I was inspired by the systemic approach of the organization in its own way seeks to find solutions in the design of new opportunities in innovative information technologies. In today's dynamic world of technology is very important to keep abreast of innovations and also need to follow the increasing pressure to secure systems against various types of attacks and risks. The amount of new information is increasing every day and way of keeping under review, at least from my perspective of system administrator is very important.

On the issue of safety information system is much more complex interdisciplinary business affair. The system safety organization must be designed with cooperation of human resources, technical means and organizational measures ensured in today's difficult times reliable information and effective protection

ZOZNAM POUŽITEJ LITERATÚRY

[1] Flickenger,R.: *Building Wireless Comunity Networks*. vyd. Boston: O'Reilly, 2003. 363 s. ISBN 0-596-00204-1

[2] Pužmanova, R.: Širokopásmový internet: *Prístupové a domáci síte*. vyd. Brno: Computer Pres, 2004. 384 s.ISBN 8025101398

[3] Pužmanova, R.: *Bezpečnost bezdrátové komunikace*. vyd. Brno: Computer Pres, 2005, 184 s.ISBN 80-251-0791-4

[4] Barken L.: *Ako zabezpečit sít WiFi*. vyd. Brno: Computer Press, 2004, 176 s.ISBN 80-251-0346-3

[5] Everts, T., Audeh,M.: The *Wireless LAN Book for Enterprises*. vyd. Canada: Trapeze Networks, 2003. 220 s.ISBN 700-9501-0001

[6] Quelet, E., Padjen, R., Pfund, A., Fuller, R., Blankenship, T.: *Building a Cisco Wireless LAN*. Vyd. USA: Syngress Publishing, 2002. 410 s.SBN 0080476244

[7] Brian Carter, Russell Shumway: *Wireless Security End to End*, Wiley Publishing, Inc., 2002 ISBN 0-7645-4886-7

[8] Frank Ohrtman, Konrad Roeder: WiFi Handbook: *Building 802.11 Wireless networks*, McGraw-Hill, 2003 ISBN 0-07-141251-4

[9] Doc. RNDr. Peter Mederly, CSc.: *Introduction to Computer Networks*, FMFI UK, Bratislava, 1997

[10] GYMERSKÁ, J. 2003. *Mechanické prostriedky a systémy technickej ochrany objektov*: Akadémia Policajného zboru v Bratislave, 2003. 111 s. ISBN 80-8054

[11] Doc. RNDr. Peter Mederly, CSc.: *Introduction to Computer Networks*, FMFI UK, Bratislava, 1997

[12] KŘEČEK, S. a kol.: *Příručka zabezpečovací techniky*. Cricetus, 2003. ISBN 80-902938-2-4.

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

WPAN (Wireless Personal Area Network) - Bezdrôtové osobné siete.

WLAN (Wireless Local Area Network) - Bezdrôtové lokálne siete.

WWAN (Wireless Wide Area Network) - Bezdrôtové rozľahlé siete.

WMAN (Wireless Metropolitan Area Network) - Bezdrôtové metropolitné siete

IEEE (Instit. of Electrical and Electronics Engineers) - Spoločnosť elektrotechnických a elektrotechnických inžinierov

BWA (Broadband Wireless Access) - Širokopásmový bezdrôtový prístup

PAN (Personal Area Network) - Osobné siete

LAN (Local Area Network) - Lokálne siete

MAN (Metropolitan Area Network) - Metropolitné siete

WAN (Wide Area Network) - Rozľahlé siete

SIG (Special Interest Group) - Špeciálna záujmová skupina

Wifi (Wireless Fidelity) - Bezdrôtová vernosť

UWB (Ultra Wide Band) - Ultra Wide Band (technológia)

TDMA (Time Division Multiple Access) - Časové delenie

P2P (Peer-To-Peer) - Spoj typu bod - bod

AP (Access Point) - Prístupový bod

SSID (Service Set Identifier) - Identifikátor bezdrôtového kanálu

DSSS (Direct Sequence Spread Spectrum) - Priama postupnosť rozprestretého spektra

QPSK (Quadrature Phase Shift Keying) - Štvorstavové kľúčovanie s fázovým posuvom

FHSS (Hopping Spread Spectrum) - Rozprestreté spektrum s preskakovanim frekv.

CCK (Complemetary Code Keying) - Doplnkové kódové kľúčovanie

CDMA (Code Division Multiple Access) - Kódové delenie prenosových kanálov

OFDM (Orthogonal Frequency-division) - Ortogonálny multiplex s kmitočtom

QoS (Quality of Service) - Kvalita služieb

BPSK	(Binary Phase Shift Keying) - Dvojstavové kľúčovanie s fázovým posuvom
QAM	(Quadrature Aplitude Modulation) - Kvadraturná amplitúdová modulácia
MIMO	(Multiple-Input and Multiple-Output) - Viac vstupov viac výstupov
WiMax	(Worldwide Interoperability for Microwave Access) - Bezdrôtová technológia
FDD	(Frequency-Division Duplex) - Frekvenčné delenie kanálov
TDD	(Time Division Duplexing) - Časové delenie kanálov
GSM	(Global System for Mobile Comunication) - Bunková telefónna technológia
UMTS	(Universal Mobile Telecommunication system) - Univerzálny mobilný telekom. system
SMS	(Short Message Service) - Krátke textové správy
DTMF	(Dual Tone Multiple Frequency) - Tonová frekvenčná voľba
GPRS	(General Packet Radio Service) - Paketový rádiový prenos dát
EDGE	(Enhanced Data rate for GSM Evolution) - Rozšírenie rýchlosti GSM prenosov
HSDPA	(High Speed Dowlink Packet Access) – Techn. vysokorýchlostného sťahovania
HSUPA	(High Speed Uplink Packet Access) - Techn. vysokorýchlostného posielania
WMM	(Wireless MultiMedia) - Bezdrôtové multimédiá
SSIM	(Service Set Identifier) - Sieťové meno
WEP	(Wireless Equivalent Policy) - Bezdrôtová kontrola
PPP	(Point to Point Protokol) - Bod po Bode
WPA	(Wi-Fi Protected Access) - WiFi chránený prístup
EAP	(Extensible Authentication Protokol) - Rozšírený autentifikačný protokol
AES	(Advanced Encryption Standard) - Pokročilý šifrovací standard
UPS	(Uninterruptible Power Supply) - Neprerušiteľný zdroj energie
ACL	(Access Control List) - Prístupová tabuľka
WNIC	(Wireless Network Interface Card) - Bezdrôtová sieťová karta
AAA	(authentication, authorization, accounting) - autentifik. autorizácia a účtovanie

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

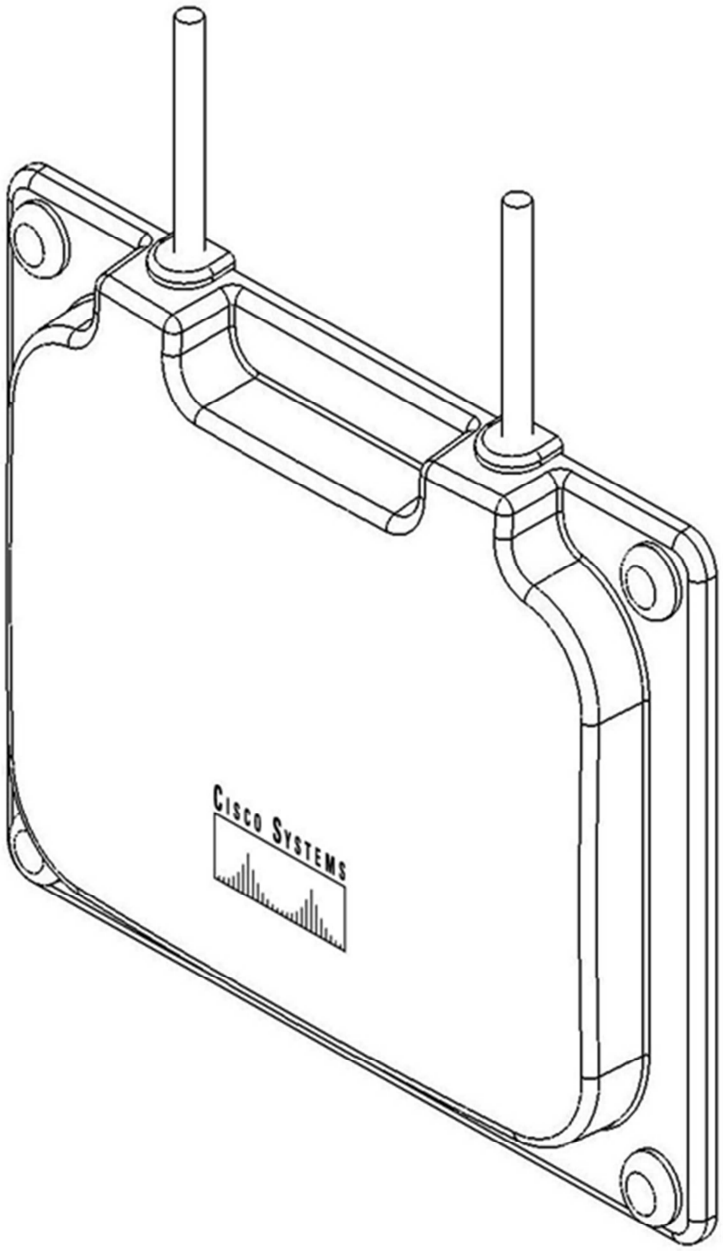
ZOZNAM PRÍLOH

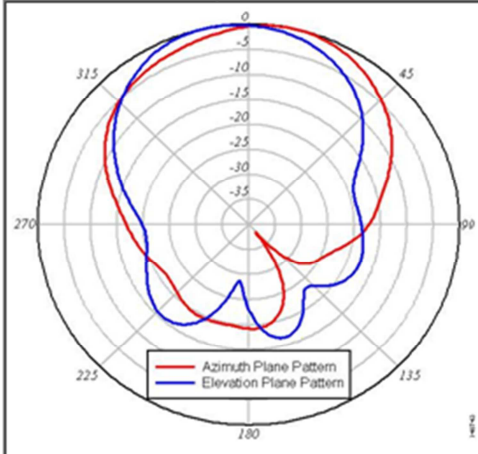
Priloha č.1 Directional anténa 6dBi

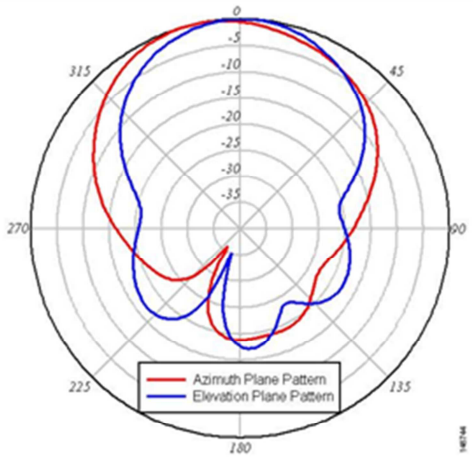
Priloha č.2 Directional anténa 8,5dBi

PRÍLOHA P I: DIRECTIONAL ANTÉNA 6DBI

Antenna type	Diversity patch
Operating frequency range	2400 - 2484 MHz
Nominal input impedance	50Ω
2:1 VSWR bandwidth	2400 - 2484 MHz
Peak gain	6 dBi
Polarization	Linear, vertical
E-plane 3-dB beamwidth	65°
H-plane 3-dB beamwidth	75°
Front-to-back ratio	15 dB
Cross-pol discrimination	15 dB
Cable length and type	36 in. (91.4 cm) Times AA-9303 or equivalent (plenum rated)
Connector type	RP-TNC
Length	4.4 in. (11.1 cm)
Width	6.6 in. (16.7 cm)
Height	1 in. (2.5 cm)
Operating temperature range	-22°F to 158°F (-30°C to 70°C)
Storage temperature range	-40°F to 185°F (-40°C - 85°C)
Environment	Indoor/outdoor







PRÍLOHA P II: DIRECTIONAL ANTÉNA 8,5 DBI

Antenna type	Single patch
Operating frequency range	2400 - 2484 MHz
Nominal input impedance	50Ω
2:1 VSWR bandwidth	2400 - 2484 MHz
Peak gain	8.5 dBi
Polarization	Linear, vertical
E-plane 3-dB beamwidth	56°
H-plane 3-dB beamwidth	66°
Front-to-back ratio	20 dB
Cross-pol discrimination	-15 dB
Cable length and type	36 in. (91.4 cm) Times AA-9303 or equivalent (plenum rated)
Connector type	RP-TNC
Length	5.1 in. (12.9 cm)
Width	5.1 in. (12.9 cm)
Height	.92 in. (2.3 cm)
Operating temperature range	-22°F to 158°F (-30°C to 70°C)
Storage temperature range	-40°F to 185°F (-40°C - 85°C)
Environment	Indoor/outdoor