

Návrh metody automatického rozložení kanálů v pásme WiFi

Bc. Tomáš Vépy

Diplomová práce
2017



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2016/2017

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Tomáš Věpy**
Osobní číslo: **A15387**
Studijní program: **N3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Forma studia: **kombinovaná**

Téma práce: **Návrh metody automatického rozložení kanálů v pásmu WiFi**
Téma anglicky: **Proposed Method for Automatic Frequency Separation in Wifi Bands**

Zásady pro vypracování:

1. Zpracujte přehled typů zařízení používaných ve WiFi sítích.
2. Charakterizujte současné možnosti správy WiFi zařízení.
3. Popište principy MESH sítí pro přístup do veřejného internetu.
4. Popište problémy spojené s kolizí WiFi sítí v pásmu 2.4 GHz.
5. Definujte narušení bezpečnosti WiFi komunikace.
6. Navrhněte způsob optimalizace rozložení kanálů WiFi sítě.
7. Odhadněte další vývoj těchto systémů.

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-80-87500-05-7
2. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management II. 1. vyd. Zlín: VeRBuM, 2012, 386 s. ISBN 978-80-87500-19-4
3. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management III. 1.vyd. Zlín: VeRBuM, 2013, 456 s. ISBN 978-80-87500-35-4.
4. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management IV. 1.vyd. Zlín: VeRBuM, 2014, 390 s. ISBN 978-80-87500-57-6.
5. KŘEČEK, Stanislav. PŘÍRUČKA ZABEZPEČOVACÍ TECHNIKY. Vydání 1. Blatná: Cricetus, 2002. ISBN 80-902938-2-4.
6. SOSINSKY, B. Mistrovství – počítačové sítě, Computer Press a.s., ISBN 978-80-251-3363-7 VÍT N., Architektura sítí, Fakulta elektrotechnika komunikačních technologií VUT Brno
7. HORÁK, J. a KERŠLÁGER, M. Počítačové sítě pro začínající správce. Brno: Computer Press, 2013. ISBN 978-80-251-3176-3.
8. CARROLL, J. B. Bezdrátové sítě Cisco. Brno: Computer Press, 2011. ISBN 978-80-251-2884-8.

Vedoucí diplomové práce:

Ing. Rudolf Drga, Ph.D.

Ústav bezpečnostního inženýrství

Datum zadání diplomové práce:

3. února 2017

Termín odevzdání diplomové práce:

24. května 2017

Ve Zlíně dne 3. února 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan



doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Jméno, příjmení: Tomáš Věpy

Název diplomové práce: Návrh metody automatického rozložení kanálů v pásmu WiFi

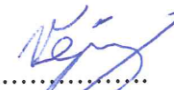
Prohlašuji, že

- 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 připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- 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/bakalářské 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, dne 24.5.2017


.....
podpis diplomanta

ABSTRAKT

Diplomová práca sa zaoberá problematikou rozloženia kanálov v bezdrôtových sieťach WiFi a pozostáva z teoretickej a praktickej časti. Je spracovaná do kapitol, ktoré rozdeľujú prácu na analýzu súčasného stavu, kde sa uvádza prehľad aktuálnych WiFi štandardov, funkcie AAA protokolu, zabezpečenie bezdrôtových sietí, protokol RADIUS, a princípy HotSpotov. V praktickej časti práce sa popisujeme postup vybudovania a nastavenia bezdrôtovej siete pomocou RADIUS serveru a HotSpotu na platforme Mikrotik.

Kľúčové slová: rozloženia kanálov, bezdrôtové siete, WiFi, RADIUS, HotSpot, Mikrotik

ABSTRACT

The diploma thesis deals with the issue of channel distribution in wireless networks WiFi and consists of a theoretical and practical part. It is crafted into chapters that divide the current state of the art analysis with an overview of current WiFi standards, AAA protocol features, wireless security, RADIUS protocol, and HotSpot principles. In the practical part of the thesis we describe how to build and set up a wireless network using RADIUS server and HotSpot on the Mikrotik platform.

Keywords: Channel layouts, wireless networks, WiFi, RADIUS, HotSpot, Mikrotik

Rád by som poďakoval vedúcemu mojej diplomovej práce pánovi Ing. Rudolfovi Drgovi, Ph.D., za profesionálne vedenie, pripomienky, pomoc a cenné rady, ktoré my poskytol pri tvorbe tejto diplomovej práce.

Prehlasujem, že odovzdaná verzia diplomovej práce a verzia elektronická nahraná do IS/STAG sú totožné.

OBSAH

ÚVOD	9
I TEORETICKÁ ČASŤ	11
1 SÚČASNÉ SPÔSOBY PRENOSU DÁT V PÁSME ISM	12
1.1 SPÔSOBY PRENOSU DÁT.....	12
1.2 PÁSMO ISM.....	14
1.2.1 Štandard Wifi	15
1.2.2 Štandard Bluetooth.....	17
1.2.3 Štandard ZigBee.....	18
1.2.4 Ostatné spôsoby prenosu.....	19
1.3 ZARIADENIA POUŽÍVANÉ VO WiFi SIEŤACH.....	23
1.3.1 Rozdelenie podľa veľkosti	23
1.3.2 Rozdelenie podľa funkčného vzťahu	25
1.3.3 Rozdelenie podľa topológie	26
1.3.4 Rozdelenie podľa technológie.....	27
1.4 SÚČASNÉ MOŽNOSTI SPRÁVY VO WiFi SIEŤACH	29
1.4.1 Autentizácia vo WiFi sieťach	30
1.5 AUTORIZÁCIE V BEZDRÔTOVÝCH SIEŤACH	31
1.5.1 Radius protokol	31
1.5.2 Autentifikácia HotSpotu.....	32
1.6 SIEŤOVÝ HARDVÉR.....	33
1.7 NARUŠENIE BEZPEČNOSTI WiFi KOMUNIKÁCIE	35
II PRAKTICKÁ ČASŤ	37
2 SPÔSOBY OPTIMALIZÁCIE WiFi SIETE	38
2.1.1 Stanovenie požiadaviek na sieť.....	38
2.2 KOMPONENTY SIETE.....	39
2.3 IMPLEMENTÁCIA WiFi SIETE	42
3 OPTIMALIZÁCIA WiFi KANÁLOV SIETE	48
3.1 KONFIGURÁCIA HOTSPOTOV.....	48
3.2 TESTOVANIE NA REÁLNYCH ZARIADENIACH A KOMPATIBILITA	49
3.3 ROZDELENIE KANÁLOV	49
3.4 CISCO CLEANAIR	53
3.4.1 Identifikácia cudzích IP	54
3.4.2 Roming.....	54
3.5 ĎALŠÍ VÝVOJ WiFi SYSTÉMOV	55
ZÁVER	57
ZOZNAM POUŽITEJ LITERATÚRY	59
ZOZNAM POUŽITÝCH SYMBOLOU A SKRATIEK	62
ZOZNAM OBRÁZKOU	64

ZOZNAM TABULIEK	65
ZOZNAM PRÍLOH.....	66

ÚVOD

Cieľom tejto diplomovej práce je popísať problematiku prevádzky bezdrôtových sietí a navrhnúť a zdôvodniť výber vhodnej metódy automatického rozloženia kanálov vo vybranom ISM pásme. Na úvod ponúkame stručný prehľad dnešných dostupných, používaných technológií v týchto sieťach a načrtneme princípy ich fungovania.

Túto tému som si v prvom rade vybral, pretože bolo mojim cieľom prehľbiť si poznatky existujúcich štandardoch v bezdrôtovej komunikácie a systémoch, prostredníctvom ktorých sa prenáša informácia a druhom rade je nestratiť prehľad v stále sa rozvíjajúcom a zdokonaľujúcom sa odvetví bezdrôtových komunikačných systémov.

V prvej časti práce sa nachádza charakteristika pásma ISM, prehľad bezdrôtových komunikačných štandardov IEEE. Ďalej tu možno nájsť prehľad aktuálnych WiFi štandardov, AAA protokol, zabezpečenie bezdrôtových sietí, protokol RADIUS, a princípy HotSpotov.

V druhej časti práce je popísaná a zdokumentovaná problematika praktického návrhu bezdrôtovej siete použitej na komunikáciu medzi niekoľkými budovami a zariadeniami vo veľkom poľnohospodárskom podniku, ktorý sa dal cestou modernizácie a využíva všetky novodobé možnosti využitia Wi-Fi, ale aj ostatné štandardy ISM.

Manažment tohto podniku pochopil že bezdrôtová komunikácia je jedným z najväčších technických prínosov ľudstvu hlavne v podmienkach kde nie je možné použiť pevné pripojenie, pretože v sebe zahŕňa prenos informácií bez potreby použitia káblov, drôtov, a iných foriem elektrických vodičov.

Dosah týchto zariadení môže byť rozličný, od niekoľkých metrov ako pri diaľkovom ovládaní, WiFi, Bluetooth, Zigbee, NFC, až po tisíce kilometrov ako je rádiová komunikácia, GSM a iné.

Existuje množstvo výhod bezdrôtových sietí na krátke vzdialenosti ako flexibilita, možnosť pokrytia iba určitého priestoru, bezproblémového pripojenie bez ohľadu na prekážky, jednoduchosť použitia ale hlavne celková cena. Medzi nevýhody bezdrôtových sietí na krátke vzdialenosti je to všeobecne, pomalšia prenosová rýchlosť, alebo slabšia odolnosť voči rušeniu.

Bezdrôtové siete sú flexibilným dátovým systémom, slúžiacim pre rozšírenie linkových počítačových sietí. Technológie používané v týchto sieťach umožňujú prepojiť počítače a ostatné zariadenia potrebné pre vybudovanie počítačovej siete.

Vzhľadom k tomu že v tejto dynamicky sa rozvíjajúcej oblasti je veľká rozmanitosť typov sieťových zariadení, pokúsime sa vybrať tú najvhodnejšiu.

Prešli sme ponuku výrobcov bezdrôtových zariadení a vybrali sme cenovo prijateľnú platformu RouterBOARD od výrobcu Mikrotik, pretože funkcie, ktoré zvláda sa vyrovnajú aj drahším zariadeniam a zároveň má širokú podporu a veľmi dobre spracované manuály pre inštaláciu. Router má v sebe integrovaný HotSpot systém, RADIUS a User Manager slúžiaci na správu pripojenia zákazníkov jednoduchú konfiguráciu a overenie realizácie.

I. TEORETICKÁ ČASŤ

1 SÚČASNÉ SPÔSOBY PRENOSU DÁT V PÁSME ISM

Pásmo Industrial, Scientific and Medical, ďalej iba ISM, je skupinu frekvenčných pásiem určená pre rádiové vysielanie využiteľné vo vedeckom, zdravotníckom a priemyselnom prostredí.

Tieto pásma sú voľné, používané v homologovaných zariadeniach bez licenčných poplatkov, čo je ich veľkou prednosťou. Čo je nevýhodou, že sú bez garancie proti rušeniu. Generálnymi licenciami vydanými telekomunikačným úradom každého štátu sú dané podmienky, platné pre používanie týchto zariadení ako je napríklad modulácia alebo maximálny výkon.

V našom prípade je Telekomunikačný úrad SR. Pásmo má hodnoty v rozsahu MHz. Bluetooth pásmo je to 2450 MHz a pásmo IEEE 802.11/Wi-Fi 2450 MHz a 5800 MHz . [1]

1.1 Spôsoby prenosu dát

Prenos dát v prípade bezdrôtových zariadení, je založený na prenose informácie rádiovým signálom alebo infračerveným lúčom. Na prenos dát je však nutná priama viditeľnosť vysielateľa a prijímateľa.

Je to rozšírenie, alternatíva káblových sietí a je to flexibilný dátový systém, ktorý umožňuje prepojiť počítače a iné zariadenia ako sú tlačiareň, terminály, alebo senzory bez použitia rozvodov.

Oblasťou použitia rozumieme blízke okolie, ktoré je vymedzené dosahom zariadenia a dosah môže byť niekoľko desiatok, maximálne stoviek metrov, v závislosti od typu zariadenia. Výhody a nevýhody bezdrôtových sietí sú:

- Mobilita.

Systémy v bezdrôtovej sieti sú charakteristické tým, že poskytujú používateľovi jednoduchý a rýchly prístup k informáciám v reálnom čase, a na akomkoľvek mieste v sieti.

- Rýchlosť a jednoduchosť inštalácie.

Inštalácia týchto zariadení je jednoduchá a rýchla a hlavným dôvodom je, že sa odstránila nutnosť inštalácie káblov. Zariadenie potrebné na inštaláciu sú komerčne dostupné a vo väčšine prípadov štandardizované.

- Prispôsobivosť.

Bezdrôtová technológia umožňuje urobiť inštaláciu siete aj tam, kde nie je možné inštalovať kábel, alebo je jeho inštalácia nie vhodná z hľadiska samotného prostredia. Všetky zariadenia sú navzájom prepojené a komunikujú spolu.

- Cena.

Bezdrôtové riešenie je v konečnom dôsledku aj cenovo efektívnejšie. Počiatočné investície sú síce vyššie ako sú náklady na pevnú sieť, ale celkové náklady na inštaláciu a tiež náklady počas ďalších životných cyklov sú nižšie.

- Variabilita pri konfigurácii.

Tieto systémy WLAN možno jednoducho konfigurovať do mnohých typov topológií tak, aby vyhovovali špecifickým požiadavkám rôznych aplikácií. Na druhej strane je tu komplikované hľadanie a odstraňovanie chýb, ako aj problematické lokalizovanie poruchy vedenia.

- Vysoká priepustnosť.

Typická prenosových rýchlostí je od 1 do 11 Mbit/s. Celková priepustnosť zariadení WLAN je však závislá od použitej technológie a topológie, ako aj od členitosti okolitého prostredia. Nevýhodou tiež je, že výkon celej siete automaticky klesá pri väčšom počte pripojených staníc.

- Využitie nelicencovaného pásma.

ISM 2,4 GHz a 5 GHz sú systémy WLAN pracujúce v medzinárodnom nelicencovanom frekvenčnom pásme. Sú spravované rádiokomunikačným úradom jednotlivých štátov a sú určené pre priemyselné, vedecké účely a pre merania a detekciu. [2]

Tabuľka 1 ISM pásma

Frekvenčné pásmo	Základná frekvencia	Dostupnosť
6.765-6.795 MHz	6.780 MHz	Potreba povolenia
13.553-13.567 MHz	13.560 MHz	
26.957-27.283 MHz	27.120 MHz	
40.66-40.70 MHz	40.68 MHz	
433.05-434.79 MHz	433.92 MHz	Len oblasť 1
902-928 MHz	915 MHz	Len oblasť 2
2.400-2.500 GHz	2.450 GHz	
5.725-5.875 GHz	5.800 GHz	
24-24.25 GHz	24.125 GHz	
61-61.5 GHz	61.25 GHz	Potreba povolenia
122-123 GHz	122.5 GHz	Potreba povolenia
244-246 GHz	245 GHz	Potreba povolenia

Spôsoby prenosu dát na malé vzdialenosti je niekoľko a malou vzdialenosťou myslíme niekoľko desiatok metrov. Medzi najznámejšie zariadenia ISM pásma patria štandardne WiFi, Bluetooth, Zig Bee a ďalšie. [3]

1.2 Pásmo ISM

Pásmo ISM je frekvenčné pásmo od 2,4 GHz po 5 GHz. Historicky k rozdeleniu jednotlivých pásiem a vyhradeniu pásma ISM došlo práve z dôvodu že vznikla potreba regulovať využitie a komerčné využitie a tiež ho obmedziť ho iba na určené frekvencie.

Predovšetkým priemysel a medicína úspešne využívajú tieto rádiové frekvenčné prenosy dát alebo energie na krátke vzdialenosti. Bezdrôtové siete ďalej možno rozdeliť z viacerých hľadísk. Všeobecne delíme pásma podľa šírky prenášaného pásma na:

- širokopásmové,
- úzkopásmové.

Podľa typu signálu sú siete:

- rádiové siete,
- infračervené siete,
- optické bezdrôtové siete.

Podľa podpory mobility delíme siete na :

- mobilné,
- pevné.

Podľa dosahu delíme siete na:

- s malým dosahom,
- so stredným dosahom. [4]

Tabuľka 2 Porovnanie niektorých bezdrôtových pripojení ISM

	802.11b WLAN (wifi)	802.15.1 WPAN (bluetooth)	802.15.4 LRWPAN (ZigBee)
Dosah	30-100 m	2-10 m	10-100 m
Prenosová rýchlosť	2-11 Mb/s	1-3 Mb/s	20-250 kbit/s
Spotreba	Stredná	Nízka	Veľmi nízka
Príklad aplikácie	Bezdrôtové pripojenie na internet	Bezdrôtové myšky, Handsfree	Bezdrôtové senzorové siete

1.2.1 Štandard Wifi

Siete WiFi, Wireless Fidelity sú siete založené na štandardoch IEEE 802.11, Institute of Electrical and Electronics Engineers. Pre objasnenie je nutné rozlíšiť označenie 802.11 a skratku Wi-Fi. Číselné označenie je číslo štandardu, ktoré prideliuje medzinárodná organizácia IEEE. Najrozšírenejšími sú štandardy 802.11a/b/g.

WiFi je označením, ktoré udeľuje Asociácia WECA, Wireless Ethernet Compatibility Alliance produktom, splňajúcim požiadavky danej normy. Každé z pásiem má odlišné vlastnosti prenosu, a preto výrobcovia podporujú naraz viacero štandardov. Pre budovanie interných bezdrôtových sietí v priestoroch, kde je inštalácia rozvodov nepraktická, alebo nerealizovateľná, sa dajú s výhodou použiť práve siete WLAN. [5]

Prvá verzia štandardu 802.11 bola publikovaná v roku 1997 a je špecifická pre prenosom dát pomocou elektromagnetického vlnenia v bezlicenčnom pásme 2,4 GHz s rýchlosťou 1 Mb/s a 2 Mb/s.

V roku 2000 sa rýchlo rozšíril WiFi štandard 802.11b pracujúca tiež v tomto pásme a stal sa najobľúbenejším spôsobom pripojenia k internetu. Pre veľký záujem o toto pásmo začalo dochádzať k prekrývaniu frekvencií a rušeniu signálu.

Táto technológia bola primárne určená pre vnútorné použitie a pre mobilitu v kancelárskych priestoroch. Postupne sa pre jej cenovú dostupnosť a nedostatok iných technológií sa stal istou náhradou služieb DSL.



Obrázok 1 Možnosti zapojenie siete WLAN, Pconfig.sk

Nezávislá základná servisná sada IBSS, Independent Basic Service Set je považovaná za nezávislú sieť, najjednoduchší variant WLAN siete. V tejto sieti je komunikácia medzi koncovými uzlami STA neobmedzená a počítače komunikujú medzi sebou v rámci dosahu vlastného sieťového adaptéra. [6]

V tejto nezávislej sade nie je žiadaná žiadna infraštruktúra, siete nie sú integrované do známych infraštruktúr, ale využívajú integráciu do sietí LAN. Nie je nutné používať prístupové body AP a pomocou externých antén sa signál dostáva do voľného priestoru, kde dokáže vytvoriť spojenie aj niekoľko kilometrov dlhé. Ak použijeme prístupový bod ako opakovač, zväčšíme dosah na dvojnásobok.

Je preto vhodná na dočasné usporiadania, ktoré trvá len krátky čas a nehodí sa pre rozsiahlejšie oblasti. [7]

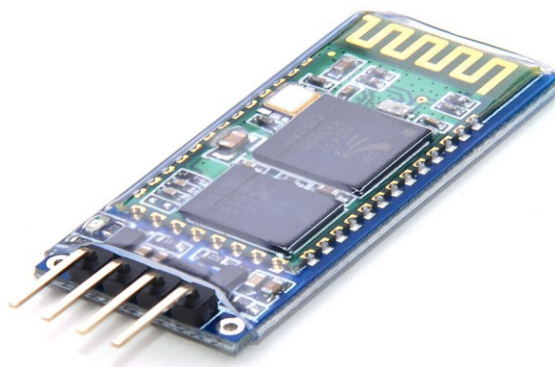
1.2.2 Štandard Bluetooth

Bluetooth je bezdrôtová technológia s krátkym dosahom, ktorá umožňuje údajovú komunikáciu medzi digitálnymi zariadeniami na vzdialenosť dnes už niekoľko desiatok metrov. Pripojenie nevyžaduje kábel a zariadenia nemusia byť k sebe otočené ako v prípade infračervenej technológie.

Vznikol ako produkt firiem 3Com, Ericsson, IBM, Intel, Lucent, Microsoft, Motorola, Nokia a Toshiba, ktorý začiatkom roku 1998 vytvorili alianciu SIG, Special Interest Group. WPAN je definovaná štandardom IEEE 802.15.1 a ide o prenos pomocou rádiového signálu v pásme ISM. Vo väčšine sveta funguje na frekvencii 2,45 GHz.

Je to prvá celosvetovo akceptovaná technológia PAN, Personal Area Network a slúži k spojeniu medzi dvoma alebo viac zariadeniami na krátku vzdialenosť v domácnosti a tiež v priemyselnom prostredí. Technológia je označená WPAN a je určené hlavne pre domácnosti, čo súvisí aj finančnou nenáročnosťou realizácie. Hoci prvé verzie neboli najlacnejšie dnes je táto technológia finančne dostupná.

Technické parametre hovoria že prenosová rýchlosť sa pohybuje okolo 720 kbit/s a zariadenie dokáže komunikovať s dvoma až siedmimi zariadeniami. Ako sme spomenuli na začiatku zariadenia nemusia na seba vidieť tak ako je to pri IrDA, infra komunikácií.



Obrázok 2 JY-MCU Bluetooth Wireless Serial

Komunikácia bola najskôr možná do 10 metrov, ale postupne sa zmenila až na vzdialenosť 100 metrov. Verzia, ktorá sa používa až do dnešnej doby, verzia 3.0, dosahuje rýchlosť až do 24 Mb/s pri použití WiFi čo sa využíva na prenos údajov. [8]

Verzia 4.0 je podobná ako 3.0, rozdiel je v tom, že je určená na prenos veľmi krátkych údajov od 8-27 bytov a s rýchlosťou 1Mb/s, zo špecifikáciou bluetooth Low Power a vyznačuje sa tým, že má veľmi nízku spotrebu energie. Dokáže pracovať až v troch režimoch spotreby a má až veľmi nízku spotrebu a v prípade potreby dokáže na batérie bežať niekoľko rokov.

Táto verzia otvorilo nové možnosti v domácnosti v zdravotníctve a v priemysle v podobe prístrojov, ktoré potrebujú komunikovať s vonkajším svetom, v rôznych senzoroch, snímačoch veličín a podobne. Napriek úspornosti dokáže táto verzia kompletne zašifrovať prenášané informácie pomocou šifrovacieho algoritmu AES, Advance encryption Standard so 128 bitovou dĺžkou symetrického kľúča.

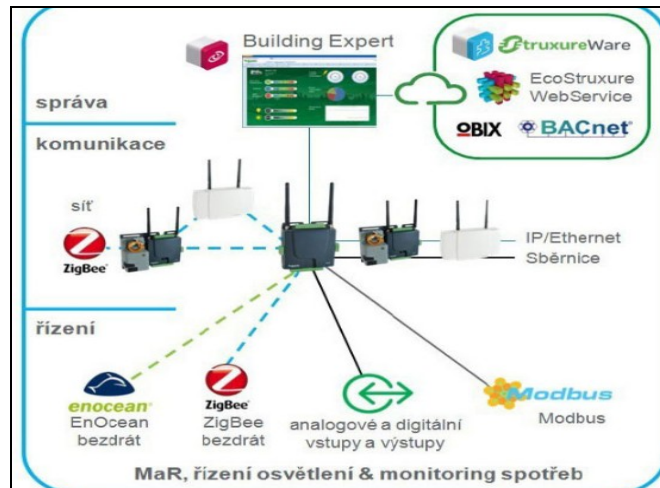
1.2.3 Štandard ZigBee

ZigBee vyvinula skupina ZigBee Alliance a je otvorený štandard, bezdrôtová senzorová sieť postavená na štandarde IEEE 802.15.4. Výhodou je že tieto prvky majú nízke požiadavky na prenosové rýchlosti a sú energeticky nenáročné v porovnaní napríklad so sieťami wifi 802.11, alebo bluetooth 802.15.1, s ktorými pracujú v pásme 2,4 GHz.

ZigBee je bezdrôtová sieť, jednoducho prístupná pre všetkých pripojených. Je to podobné ako bluetooth, ale tento je skôr využívaný v spotrebnej elektronike. ZigBee vznikol špeciálne pre priemyselné aplikáciách pre ktoré nebol Bluetooth vhodný.

ZigBee sa zameriava na bezdrôtovú komunikáciu špeciálne v priemyselnej automatizácii a uzly siete môžu tvoriť FFD zariadenie, čo sú plne funkčné zariadenia, vykonávajúce funkcie ako koordinátor, smerovač alebo koncové zariadenie. [9]

Okrem funkcie pripájania rôznych počítačových periférií našli uplatnenie hlavne pri automatizácii a regulácii v budovách a priemyselných prevádzkach, pri riadení klimatizácia, osvetlenia, ako rôzne snímače alebo zabezpečovacia technika. Tiež sa používa v spotrebnej elektronike ako diaľkové ovládače a všetkých možné zariadenia v domácnosti, ktoré sú vybavené nejakou riadiacou elektronikou.



Obrázok 3 iBMS systém SmartStruxure, sbs.sk

Má veľmi dobré vlastnosti, čo sa týka hlavne energetickej náročnosti, má schopnosť opraviť spojenie v prípade ak nejaký prvok v sieti vypadne, je technologicky jednoduchý, flexibilný a nepotrebuje konfiguráciu čo, umožňujú nasadenie aj do domácnosti.

Flexibilita spočíva v schopnosti detekovať existujúce siete a prístup prvku k tomuto zariadeniu trvá okolo 30 ms. [10]

1.2.4 Ostatné spôsoby prenosu

Okrem týchto často používaných významných štandardov existujú ešte omnoho viac aj keď nie tak často používaných spôsobov a to napríklad:

Pásmo 433 a 868 Mhz

Jedným zo spôsobov je pásmo 433 a 868 Mhz. Je obľúbené pre prenos malých objemov dát, ale nepresadil sa tu žiadny významnejší štandard. Prenosové rýchlosť sa pohybuje od 4 Kbps do 128 Kbps a prenosová vzdialenosť môže byť až 800 metrov. Pásmo používajú lacnejšie myši a klávesnice, bytové senzory, detské hračky na diaľkové ovládanie.

Typickou aplikáciou je nahradenie sériovej komunikácie, v prostrediach kde už existuje niekoľko RF sietí postavených v pásme 2,4GHz prípadne 868 MHz. Ich výhodou je nízka cena a použiteľnosť tohto pásma na celom svete a problémom môže byť vzájomné rušenie.

Štandard NFC

NFC, Near Field Communication je v skratke je krátko dosahové, bezdotykové, vysoko-frekvenčné prepojenie, ktoré dovoľuje výmenu dát medzi zariadeniami do vzdialenosti okolo 4 -10 cm.

Táto skratka, sa začala objavovať vo svete koncom roku 2003 rozšírením štandardu ISO/IEC 14443, ako bezkontaktné karty RFID, ktoré kombinujú rozhranie smart kariet a čítačiek do jedného zariadenia a ktorú možno nájdete aj v nastaveniach vášho smartfónu.

V roku 2004 spoločnosti Nokia, Philips a Sony založili NFC Forum, ktoré tvorí základ pre sledovanie trendov, popis technológie a základné špecifikácie pre NFC. Prvé testy technológie začali s telefónom Nokia v roku 2006 vo Veľkej Británii.

Dôležitý bol rok 2009. NFC Forum vydalo Peer-to-Peer štandard ktorý slúži na prenos kontaktov, URL adries a spustenie Bluetooth technológie. Samsung Nexus je prvý smartfón so zabudovanou technológiou NFC a o tri roky neskôr Samsung uzavrel zmluvu o spolupráci so spoločnosťou VISA o vývoji nového spôsobu platby.

NFC má niekoľko foriem a jednou z nich sú dnes napríklad bezkontaktné mobilné platby, ktoré sa vyvinul z mobilných aj bezkontaktných platobných systémov v minulosti. Akékoľvek zariadenie je schopné vykonávať platby pomocou identifikácie. Hovoríme o RFID rádiových technológiách, ktoré využívajú bezkontaktnú platobnú technológiu. Najčastejšie používaný prístroj pre bezkontaktné platby je smartphone. Anténa aj čip vložený do zariadenia umožňuje zákazníkovi použiť smartphone cez čítačku kariet.

Zabezpečenie pre bezkontaktné platby je rovnaká ako u kreditnej karty. Pre posielanie informácií slúžia zabezpečené kanály a šifrovanie. Výhodou je že typicky bezkontaktné platby sú rýchlejšie, pretože nie je nutná číslo PIN ani podpis. [11]

Štandard Wierelles – Mbus

V dnes sa do popredia dostávajú zariadenia, ktoré nie sú závislé na káblovom prepojení medzi prijímačom a vysielačom. Preto je M-Bus aliancia nový bezdrôtový štandard, označovaný aj ako W-MBus.

Mbus je technológia, ktorá nevyužíva rádiovú komunikáciu, ale využíva komunikáciu pomocou dvoch káblov. Používa systém, ktorý schválila Európska norma, EN 13757-2 fyzickej a linkovej vrstvy a pre STN EN 13757-3 aplikačnej vrstvi.

Bezdrôtový M-Bus je definovaný štandardom EN 13757-4:2005 a norma hovorí o prenose dát napríklad medzi vodomermi, elektromermi, meračmi tepla, plynu, s centrálnou databázou a vyhodnocovacím alebo riadiacim systémom. Hlavne sa používa v systémoch určených na automatické odčítanie dát pri spotrebe energií, známej ako AMR systémy v domácnostiach a v priemyselných oblastiach. [12]

WM-bus sa potom realizuje namiesto prenosu po dvojici káblov, bezdrôtovým prenosom v pásme ISM s frekvenciou 868 MHz a to v rámci sieťovej komunikácie niekoľkých jednotiek. Tento systém tvorí v Európe akceptovaný základ nových AMI, Advanced Metering Infrastructure ištaláci.

Štandard KNX – RF

Požiadavky na technické zariadenie budov sa neustále zvyšujú. Štandard KNX je medzinárodný štandard pre inteligentné elektrické inštalácie, ktoré postupne nahrádzajú tradičné elektrické inštalácie. KNX je oficiálne prvým celosvetovým štandardom pre technológie automatizovaného riadenia.

Je nástupcom predchádzajúcich troch noriem EHSP, European Home System Protocol, BatiBus a EIB, European Installation Bus. KNX je spravovaný KNX Alianciou a podporovaný výrobcami ako sú ABB, Jung, Gira, Merten, Schneider Electric, Siemens a ďalší.

Pohodlie a zároveň efektívne využitie energie, teda nižšiu spotrebu energie je možné dosiahnuť práve inteligentným riadením a snímaním všetkých produktov. To by znamenalo viac pripojených vodičov od snímačov k riadiacim centráram, čo je neprípustné a odpoveďou je práve KNX.

Systém má odstrániť problémy s izolovanými prístrojmi a zabezpečiť, aby všetky komponenty komunikovali spoločným jazykom, systém, kde aplikácie zdieľajú nezávislé KNX zbernice.

Cez médium KNX, ku ktorému sú pripojené zbernicové prístroje ako snímače alebo akčné členy potrebné pre riadenie technického vybavenia budovy si môžu zariadenie vymieňať informácie. Zbernicovými prístrojmi sú osvetlenie, tienenie, bezpečnostné systémy, vykurovanie, klimatizačné systémy, signalizácia a monitorovanie, audio a video technika alebo biela technika.

Všetky tieto funkcie je možné riadiť, monitorovať a signalizovať jednotným systémom bez ďalších nadbytočných riadiacich centier a štandard je založený na komunikačnom zásobníku EIB, plus sa rozšíril systém o fyzické vrstvy, konfiguračne režimy a aplikačne vlastnosti BatiBus, EHS.

KNX býva štandardne riadené 8-bitovým mikrokontrolérom v PC, záleží od konkrétneho prevedenia. Projektant však má pri výbere KNX technológie k dispozícii štandardizované, medzinárodne uznávané riešenia. KNX – RF je bezdrôtová verzia štandardu KNX. [13]

Štandard IQRF

IQRF bezdrôtová technológia, ktorá láme bariéry. A to hlavne z dôvodu jednoduchej inštalácie. Inteligentnú bezdrôtovú technológiu IQRF je možné inštalovať so základnými znalosťami elektroniky v rekordne krátkom čase. Inteligentné budovy alebo prenos dát, sú len niektoré z príkladov použitia týchto moderných technológií IQRF. [14]

Technológia IQRF má niekoľko alternatív ale najvhodnejšie je 4. alternatíva, ktorá je prakticky okamžite použiteľná s pomocou protokolu DPA Direct Peripheral Addressing, ktorý umožňuje vytvárať, ovládať a modifikovať veľké drôtové a bezdrôtové siete a prenášať dáta obojsmerne bez programovania.

Základom celého systému IQRF sú miniatúrne RF vysielače, pracujúce na frekvencii 868 MHz alebo 916 MHz s veľmi nízkou spotrebou a nastaviteľným RF výkonom. Celé nastavenie a pripojenie siete prebieha automaticky.

IQRF má nízky výkon, nízke rýchlosti a nízky objem dát a bezdrôtová konektivita je v rozmedzí desiatok až stovky metrov v sieťach napríklad pre telemetriu, priemyselné riadenie a automatizáciu časti budov a miest. Dá sa použiť s akýmkoľvek elektronickým zariadením, ak je potreba bezdrôtového prenosu, diaľkové ovládanie, monitorovanie na diaľku alebo pripojenie zariadení k bezdrôtovej sieti.

Vnútorý MCU je vybavený operačným systémom IQRF OS, ktorý využíva bezdrôtovú komunikáciu, siete Mesh a ďalšie funkcie. Ďalšia funkčnosť je daná implementovaným softvérom umiestneným do rovnakého interného MCU.

Smerovanie, šírenie paketov v sieti je možné buď koncovými TR na pozadí, alebo prostredníctvom vyhradených smerovačov. Pri pokuse o pripojenie k zložitým štandardom sú k dispozícii lokálne USB alebo vzdialené GSM, Ethernet alebo WiFi brány.

Táto brána môže tiež slúžiť ako datalogger a bude transparentne zhromažďovať dáta z koncových zariadení. Najdôležitejšie pripojenie k vzdialenej bráne je cez IQRF Cloud, ktorý poskytuje plug-and-play celosvetový prístup ku koncovým zariadeniam.

Implementácia IQRF je jednoduchá najmä vďaka sofistikovanému konceptu s operačným systémom a DPA a aj kvôli vysoko účinným vývojovým nástrojom ktoré umožňujú rýchly vývoj. IQRF IDE poskytuje všetky funkcie pre vývoj, servis a údržbu. [15]

1.3 Zariadenia používané vo WiFi sieťach

Prakticky každá moderná domácnosť, firma, škola, inštitúcia alebo aj dopravný prostriedok, je dnes pripojený k internetu alebo do vlastnej počítačovej siete. Dostupnosť internetu na Slovensku dosahuje takmer Európsky priemer. Ľudia si zvykajú, aj keď asi 15 percent populácie vo veku 16 až 74 rokov nikdy nepracovala s internetom.

V roku 2005 nemalo žiadne skúsenosti s internetom až 42 percent Slovákov v tomto veku v roku 2013 ho už malo internet podľa najnovších štatistík až 78 percent domácností a asi 61 percent Slovákov surfuje denne, čo podľa odborníkov prinieslo výrazné zlacnenie a dostupnosť výpočtovej techniky a lepšie pokrytie. [16]

Preto je dôležité poznať rôzne kategórie, ktoré majú určité vplyv na rozširovanie počítačových sietí. Môžeme ich kategorizovať podľa viacerých kritérií

1.3.1 Rozdelenie podľa veľkosti

PAN, Personal area network, je malá osobná sieť, ktorú spravidla využíva len jedna osoba na prepojenie mobilu, počítača, PDA, notebooku a spája zariadenia rádovo v dosahu niekoľkých metrov.

WPAN bezdrôtová osobná počítačová sieť je osobná počítačová sieť - sieť na prepájanie zariadení so zameraním na pracovný priestor jednotlivca - v ktorom sú bezdrôtové pripojenia. Je založený na štandardnom IEEE 802.15. a dva hlavné druhy bezdrôtových technológií, ktoré sa používajú pre protokol WPAN, sú Bluetooth a Infračervené dátové združenie ako bezdrôtové technológie (WiFi, IrDA, BlueTooth).

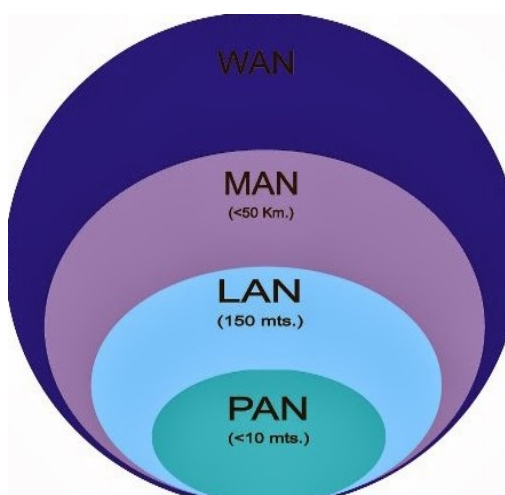
LAN, Local Area Network, je lokálna počítačová sieť, prepojenie dvoch alebo viacerých počítačov so vzájomnou možnosťou komunikácie a so spoločným využívaním zdrojov ako sú disky, tlačiarne, softvér pre tieto prepojené počítače. Je typická pre sieť ktorá spája nie-

koľko susedných miestností v jednej budove alebo najviac v jednom bloku budov. LAN sú väčšinou pod správou súkromnej spoločnosti a sú tvorené káblovým systémom alebo iným prenosovým médiom WIFI, FDDI.

LAN zahŕňa káble, prepínače a smerovače, ktoré umožňujú užívateľom pripojiť sa k interným serverom, webu alebo do ďalších lokálnych sietí prostredníctvom siete WAN. Ethernet a Wi-Fi sú základné spôsoby, ako pripojiť LAN. Ethernet je špecifikácia, ktorá umožňuje počítačom komunikovať medzi sebou navzájom a Wi-Fi využíva rádiové vlny na prepojenie počítačov do siete LAN.

MAN-Metropolitan area network, je určená na prepájanie lokálnych sietí v mestskej zástavbe a obvykle je obmedzená na jedno mesto s počítačovými zdrojmi v zemepisnej oblasti alebo regiónu. Spája na vzdialenosť rádovo desiatky kilometrov. Nasleduje prepojenie do siete Wide Area Network.

WAN-Wide area network je charakteristická tým, že spája rôzne LAN a MAN siete v pôsobnosti krajín, kontinentov a sveta. Wide Area Network je prepojením niekoľkých lokálnych sietí, podľa ich dôležitosti, vzájomne prepojených s chrbticovou linkou. Je tiež niekedy označovaná ako univerzitná sieť. Rozľahlé siete umožňujú komunikáciu na veľké vzdialenosti. Obvykle bývajú verejné, ale existujú aj súkromné WAN siete. [17]

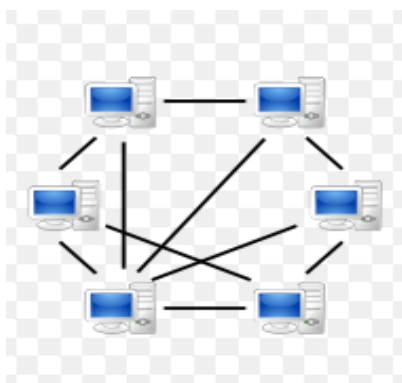


Obrázok 4 Rozdelenie sietí podľa veľkosti

1.3.2 Rozdelenie podľa funkčného vzťahu

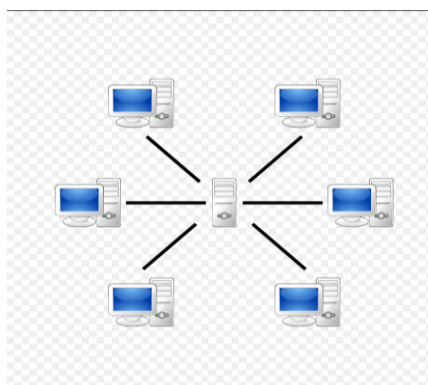
Ďalej rozdeľujeme siete, podľa funkčného vzťahu a to je vzťah, pri ktorom záleží na tom, ako spolu komunikujú klienti, či komunikujú priamo alebo pomocou sprostredkovateľa, ktorým je server. Potom ich delíme na:

- Klient-server a tu služby poskytuje staniciam server, workstation, pracovná stanica je klient. Existuje niekoľko typov serverov, podľa toho aké poskytuje služby. Je to napríklad súborový server, tlačový server, poštový server, www server, ftp server a ďalšie. Neplatí však vzťah, že jeden server je jeden počítač.



Obrázok 5 Zapojenie PC klient - server

- Peer-to-peer je pomenovanie ktoré vyjadruje vzťah rovný k rovnému a označujeme ho aj ako P2P sieť. Ktorákoľvek stanica v sieti môže vyhradiť nejaký prostriedok ako napríklad diskový priestor, tlačiareň, alebo mechaniku na zdieľanie a iná stanica môže tento využívať. Obvykle tento typ siete nemá centrálnu správu, pretože každý uzol sa spravuje sám a prostriedky je možné zdieľať cez internet.



Obrázok 6 Zapojenie PC Peer-to-peer

1.3.3 Rozdelenie podľa topológie

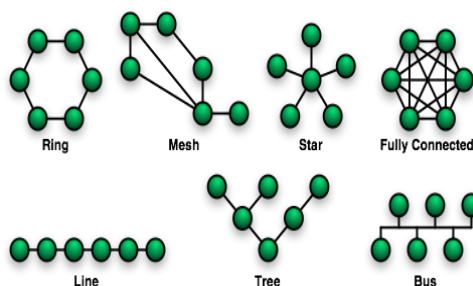
Topológia siete je vlastne architektúra počítačovej siete alebo systém usporiadania, akým sú počítače a iné zariadenia v sieti pospájané medzi sebou. Poznáme dva spôsoby, ako definovať geometriu siete, fyzická a logická topológia.

Fyzická je skutočné geometrické usporiadanie pracovných staníc. Existuje niekoľko bežných, ako je popísané nižšie a znázornené na obrázku.

Logická topológia sa vzťahuje k povahe ciest signály ktorý ide z uzla do uzla. V mnohých prípadoch je logická topológia je rovnaká ako fyzickej topológii. Ale nie vždy.

Hlavnú úlohu vždy zohrávajú aktívne prvky, ktoré majú za úlohu prepájať samostatné časti sietí, komunikujú medzi klientmi, ochraňujú pred neželaným prienikom a riadia sieť aby nedošlo ku kolíziám. Sieť môže byť prepojená z počítača do počítača alebo častejšie s využitím aktívnych členov.

- Zbernicová topológia, Bus topology je spôsob pripojenia počítačov do počítačovej siete. Spojenie predstavuje jediné prenosové médium ktorým je zbernica, ku ktorej sú pripojené všetky uzly siete ktoré predstavujú koncové počítače
- Hviezdicová topológia je najčastejšie používaný typ topológie siete. V nejednoduchšej forme sa skladá z jedného centrálného uzla, ktorý sa skladá z prepínača, rozbočovač, smerovača alebo je to jeden počítač, ktorý sa správa ako niektoré z týchto zariadení.
-



Obrázok 7 Topológia sietí

- Kruhová alebo prstencová topológia, označuje zapojenie, v ktorom je jeden uzol pripojený k ďalším dvom uzlom tak, že tvoria kruh.
- Ďalšia topológia je hviezda. Rozdiel medzi prstencovou topológiou a hviezdou je, že je menej efektívna a pomalšia ako hviezdicová sieť. Dôvodom je že v nej musia dáta prejsť cez veľké množstvo uzlov kým sa dostanú k cieľu. [18]

1.3.4 Rozdelenie podľa technológie

Poznáme niekoľko druhov technológií, ale pre získanie prehľadu by sme stručne popísali týchto päť technológií ktoré sa využívajú hlavne v počítačových sieťach.

ARCNET

ARCNET, Attached Resource Computer je technológia vyvinutá firmou Datapoint v roku 1976, ktorá sa rýchlo stala jednou z najrozšírenejších pre výstavbu lokálnych sietí. Má stromovú topológiu a všetky stanice v sieti sú prepojené opakovačmi. Pôvodne boli opakovače prepojené úsekmi koaxiálneho kábla s presnou špecifikáciou parametrov, čo platí aj pre vzájomné prepojenie opakovačov.

Okrem stromovej topológie dnes už niektorí výrobcovia dovoľujú aj zbernicovú topológiu a používajú sa symetrické káblov aj optické vlákna. V roku 1990 bola na trh uvedená modifikácia technológie pod názvom Advanced ARCNet, ktorá používa modernú šesnásťkovú fázovo-amplitúdovú moduláciu a dosahuje rýchlosť prenosu 20 Mb/s.

Token-ring

Technológia Token-ring bola vyvinutá firmou IBM v sedemdesiatych rokoch, ešte pred tým ako vznikla myšlienka prepájať počítače medzi sebou a nástupom osobných počítačov. Neskôr keď vznikla takáto požiadavka, boli tieto technológie predložené spoločnosti IEEE ktorá si Token Ring zriadila ako samostatnú podskupinu 802.5. a prijala toto riešenie navrhnuté firmou IBM ako svoj štandard.

Rýchlosti prenosu siete Token ring sú 4 Mbit/s, 16 Mbit/s, 100 Mbit/s a 1 Gbit/s a sú štandardizované IEEE 802.5. Postupne technológia Token-ring začína upadať. Zaostáva čo do výkonu, spoľahlivosti, ale aj v cene, pred technológiu Ethernet.

100VG-AnyLAN

Technológia bola vyvinutá firmou Hewlett-Packard, za príspevku niektorých ďalších firiem s ambíciami stať sa ďalším vývojovým štádiom klasického 10 megabitového Ethernetu. Mal to byť rozdiel medzi dvoma smermi a odlišovať sa mal v prístupovej metóde, riešajúcej súbeh žiadostí na vysielanie od jednotlivých uzlov.

Autori technológie chceli dosiahnuť že nedeterministická pôvodná prístupová metóda je prežitok a už nie je nevyhnutná a je lepšie ju nahradiť inou prístupovou metódou, schopnou lepšieho využitia zmenených podmienok, technológiou 100VG-AnyLAN ktorá je pokročilejšia a lepšia ako 100 megabitový Ethernet (100BaseT)

Má lepší výkon pri väčších záťažach, ale tiež veľmi dobré možnosti riadenia a obrany proti narušeniam. Napriek výhodám sa zatiaľ nepodarilo tejto technológii 100VG-AnyLAN oproti technológii Ethernet presadiť.

FDDI

FDDI je prenosová technológia na úrovni linkovej vrstvy ale zasahuje aj do vrstvy fyzickej pretože si môže sama definovať konkrétny spôsob využitia svojho prenosového média, na úrovni fyzickej vrstvy. Od začiatku počíta s využitím optických vlákien a vďaka tomu dokáže ponúknuť podstatne väčší dosah než ostatné prenosové technológie.

Kruh, do ktorého sú jednotlivé stanice prepojené, môže mať obvod až 200 km, a môže v ňom byť zapojených až 500 uzlov. Prenosová rýchlosť je až 100 Mbps, čo do značnej miery predurčuje spôsob nasadenia technológie FDDI ako chrbticovej prenosové technológie, ktorá prepája medzi sebou výkonné servery a aktívne prvky v rámci veľkých celkov.

FDDI je jedna z najstarších vysokorýchlostných prenosových technológií, ktoré využívajú vysoké prenosové výhody optických vlákien, ale jej cena ostáva naďalej veľmi vysoká. A preto je často nahradená technológiou Fast Ethernet, ktorá ponúkla 100 Mbps rýchlosť za oveľa nižšiu cenu.

Ethernet

Jedným z najhlavnejších popisovaných technológií je Ethernet. Ethernetu sa vývíjal pri výhradne v rámci IEEE. Štandardy IEEE tento vývoj v zásade iba kopírujú. Ethernet bol pôvodne vyvinutý ako pioniersky projekt v spoločnosti Xerox PARC v roku 1973, keď Robert Metcalfe popísal potenciáli Ethernetu.

Dáta sú prenášané v základnom pásme v kóde Manchester, rýchlosťou 10 Mb/s a kľúčová je pre Ethernet je zbernicová topológia a prístupová metóda CSMA/CD (Carrier Sense with Multiple Access and Collision Detection. Ktorá je pri prístupe k médiu je veľmi efektívna pri nižšom zaťažení siete čo je asi 30% šírky pásma. Efektivita klesá pri väčšom počte záujemcov o vysielanie. Ethernet technológia patrí medzi najrozšírejšie a najpoužívanejšie technológie a ešte dlhú dobu bude patriť, čo do výkonu, spoľahlivosti, ale aj v cene

1.4 Súčasná možnosti správy vo WiFi sieťach

Dosiaľ sme popisovali skôr hmatateľné súčasti siete, ale rozsiahle siete je nevyhnutné zabezpečovať a spravovať, čo môžeme zhrnúť pod skratku protokolu AAA. AAA znamená tri neodmysliteľné funkcie, autentifikácia, autorizácia a účtovanie teda accounting. Skratka je pri zabezpečení veľmi často používaná, pretože v infraštruktúre je veľmi dôležité overovať používateľa. [19]

Tento protokol je využívaný hlavne na zabezpečenie siete voči používateľovi do nej prístupujúcemu. Protokol prideluje, alebo zakáže prístup k prostriedkom a pomáha administrátorom nastavovať práva či oprávnenia používateľa. [19]

Účtovanie teda accounting pomáha sledovať, ktoré prostriedky, kto a ako využíva a zariadenie ktoré toto sleduje je autentizačný server. V praxi sa dnes častejšie využíva riešenie AAA serveru, ktorý kombinuje autentizáciu, autorizáciu a účtovanie. Pre riadenie prístupu do siete sú tieto funkcie známe ako centralizované riešenie.

AAA server je vždy v infraštruktúre implementovaný ako samostatné zariadenie a nie je súčasťou iného sieťového prvku. V súčasnej dobe sa využíva väčšinou jeden z troch autentizačných protokolov. Postupne popíšeme náležitosti samotného AAA protokolu a potom sa zameriame na protokol RADIUS.

Najrozšírenejším protokolom je RADIUS, od spoločnosť Lucent. Ale pomerne rozšíreným protokolom je protokol TACACS+ vyvinutý firmou Cisco alebo protokol Diameter ktorý vychádza z protokolu RADIUS, ale má podstatné odlišnosti a s RADIUS-om nie je kompatibilný. [20]

1.4.1 Autentizácia vo WIFI sieťach

Autentizácia aj v bezdrôtových sieťach proces posudzovania, pri ktorom sa zvažuje či je zariadenie na sieti alebo používateľ, ktorý požaduje prístup je oprávneným používateľom. Pri tomto procese sa posudzuje identita používateľa a jeho ďalšie údaje, najčastejšie heslá a digitálne certifikáty. Ak je autentizácia úspešná, používateľovi je povolený prístup do siete.

Ako sme už niekoľko krát spomenuli bezdrôtové siete sú dnes všade okolo nás. V lokalitách, kde sa stretáva väčší počet ľudí, budujú sa verejné prístupové body HotSpoty, ktoré zabezpečujú pripojenie na letiskách, železničných staniách, halách.

Bezdrôtové siete, ako už vieme sú založené na štandarde IEEE 802.11. a najznámejšími štandardmi sú 802.11a/b/g a ako už vieme, každé pásmo má iné vlastnosti prenosu, hoci výrobky známych výrobcov podporuje aj viacero štandardov naraz.

Toto je dôležité aj preto, že skôr než sa môže začať akákoľvek komunikácia medzi klientom a prístupovým bodom v bezdrôtovej sieti. Zariadenia, ktoré zabezpečujú dialóg musia tento dialóg začať. Hovoríme tomu pridruženie, asociácia.

V návrhu normy 802.11 sú funkcie ktoré zabezpečujú že sieť môže vyžadovať autentizáciu klienta, ktorá musí prebehnúť okamžite po jeho pridružení, a pred začiatkom vysielania z prístupového bodu. Toto všetko je zvlášť dôležité v bezdrôtových sieťach ak sa zvažuje, či je zariadenie alebo užívateľ legálnym používateľom siete. [21]

Ak je autentizácia úspešná užívateľovi alebo zariadeniu je následne umožnený prístup do siete. Takto prebieha Autentifikácia celý proces overenia identity a existuje niekoľko druhou spôsobov ako autentifikovať. Medzi tieto spôsoby patrí napríklad:

- Open system,
- Filter MAC adres,
- Wep-Shared Key,
- WPA PSK,
- WPA 2,
- Autentizačná metódy EAP. [22]

1.5 Autorizácie v bezdrôtových sieťach

Prístup do siete je proces ktorý je vo väčšine počítačových systémov zabezpečený v dvoch krokoch. Na autentizáciu je nadväzuje autorizácia, ktorá začína po úspešnej autentifikácii. Overený používateľ musí následne mať povolenie na vykonanie požadovaných operácií.

Bežný užívateľ nemá možnosť prístupu ku všetkým častiam systému. Autorizácia sa zaisťuje pomocou zoznamov, ACL alebo zásad, ktoré určuje politika vlastníka siete. Pomocou týchto zásad môže administrátor kontrolovať úroveň prístupu používateľa, ak sa užívateľ úspešne prihlásil. [23]

Tieto individuálne stupne povolenia je možné pridelovať lokálne alebo cez vzdialený server. Pomocou autorizácie je možné zabezpečiť to, aké typy aktivít má klient povolené, napríklad :

- Umožňuje využívať služby Quality of Service napríklad hlasové, video a podobne,
- Je možné obmedziť určitú dobu na poskytovanie služby.
- Povoľujeme typy komunikácie, medzi ktoré patrí napríklad FTP alebo WWW.
- Môžeme povoliť prístupy užívateľovi do špecifických častí siete.
- Je možné obmedziť množstvo prenesených dát.
- Pridelujeme adresy vždy iba z určitého rozsahu adries.
- Môžeme pri nej určiť maximálnu alebo minimálnu prenosovú rýchlosť siete. [24]

1.5.1 RADIUS protokol

Protokol ktorý použijeme v praktickej časti práce je ako sme spomínali protokol RADIUS. Tento protokol je špecifikovaný dokumentom RFC-2865 a jeho úlohou je centralizovať autentizáciu používateľa.

Tento protokol funguje tak, že ak sa používateľ pripojí k serveru, tento server preverí oprávnenia a umožní alebo zamietne prístup klienta do siete. Najčastejšie je dnes NAS server ale môžeme použiť hocijaké zariadenie, ktoré podporuje protokol RADIUS klient, ktorý obsahuje smerovače alebo switche.

RADIUS je centralizované preverovanie používateľa prístupujúceho do siete. Protokol neoveruje práva používateľa ale zabezpečuje komunikáciu medzi RADIUS serverom a

NAS serverom. RADIUS server obsahuje niekoľko autentizačných mechanizmov a informuje či je povolený prístup klienta a ak áno, za akých podmienok.

Tento protokol využíva UDP, User Datagram Protocol čo je datagramová služba ako DNS, Domain Name System, a hlavným dôvodom výberu tohto protokolu je nutnosť rýchlejšej odozvy na požiadavky pri prihlásení používateľa.

Radius je teda komplexný overovací systém, ktorý obsahuje veľké množstvo autentizačných mechanizmov, ktoré sa dajú využiť na overovanie pomocou používateľského mena a hesla a to použitím protokolu PAP, Password Authentication Protocol.

Princípy takejto RADIUS autentizácie a autorizácie spočívajú v tom, že používateľ poskytne NAS svoje autentizačné informácie, čo sú používateľské meno a heslo. NAS server, vytvorí správu Access-Request, ktorá všetko toto obsahuje.

Takto vložené heslo je zašifrované pomocou algoritmu RSA, Message Digest Algorithm MD5 a správa je následne odoslaná do príslušného serveru. Správa odosiela opakovane ak od serveru nepríde odpoveď a po určitom počte opakovaní sa posunie na ďalší NAS server.

Ak je požiadavka prijatá server skontroluje, či má tajný kľúč k NAS serveru, od ktorého požiadavka prišla. Ak kľúč neexistuje, požiadavka je zamietnutá a zamietnutie požiadavky je zaznamenané na serveri. Ak existuje v databáze kľúč, požadované používateľské meno na daný účet sa otvorí používateľovi podľa daných údajov.

RADIUS accounting slúži tak ako sme už spomínali všeobecne k zaznamenaniu informácií o prihlásení a odhlásení používateľov a týmto protokolom sa sleduje ako a kedy bol zákazník prihlásený, koľko dát preniesol a ako dlho bol prihlásený.

1.5.2 Autentifikácia HotSpotu

Špeciálna je autentifikácia k HotSpot-u, čo je všeobecne označovaná oblasť, kde je možné sa prihlásiť za pomoci bezdrôtovej technológie WiFi a pripojiť sa k intranetu alebo k Internetu tak ako sa budeme pripájať my v našej praktickej časti. [25]

Hotspot je v podstate chápaný ako služba, ktorá po autentizácii používateľa umožňuje prístup do Internetu. Výhodou tejto služby je, že tu nie je potrebná žiadna inštalácia softvéru alebo vybavenie na to aby sme sa mohli okamžite pripojiť. [26]

Komunikácia prebieha na strane používateľa cez webové rozhranie prehliadača a HotSpot sa vie pripojiť na každé zariadenie, ktoré používa jednoduchý webový prehliadač.

HotSpot-y sú využívané na miestach kde je množstvo ľudí.

Po pripojení zariadenia k HotSpotu mu tento prideli IP adresu. IP adresu prideliuje DHCP server, ktorý je na tej istej lokálnej sieti ako je HotSpot. Používateľské zariadenie požiada si o pridelenie IP adresy a DHCP server poskytne jednu z voľných IP adries. Používateľ sa prihlási a následne sa otvorí prehliadač.

Používateľ zadá prihlasovacie meno a heslo a HotSpot brána toto porovná so svojou databázou. Ak sú údaje zhodné, Hot Spot používateľovi povolí prístup do miestnej siete alebo internetu. Používateľ následne môže zadať požiadavku na internetovú stránku. [27]

1.6 Sieťový hardvér

V praktickej časti budú použité rôzne hardvérové prvky ktoré sa líši podľa aktuálnych potrieb a nárokov kladených na sieť či už na strane správcu siete alebo používateľa. Na trhu je široký sortiment Wi-Fi zariadení, ktorý dokáže pokryť väčšinu nárokov.

V praktickej časti sa zameriame na konkrétny prvok, ale pre oboznámenie sa budeme venovať aj stručnému prehľadu a popisu vlastností v nasledujúcom texte. Základné rozdelenie hovorí o aktívnych a pasívnych WiFi hardvérových prvkoch.

Medzi aktívne WiFi komponenty na strane používateľa patria karty typu PCI. Sú to vlastne Wi-Fi adaptéry, inštalované priamo do PCI slotu počítača, obsahujúce malú anténu, ktorá sa dá nahradiť externou anténou. Pokiaľ na treba na takomto adaptéri urobiť spoj na väčšiu vzdialenosť v exteriéri, tak je vhodné použiť dodatočnú anténu.

Výhodou Wi-Fi adaptérov je nízka cena a medzi nevýhody patrí hlavne riadenie karty operačným systémom PC, ktorý je u väčšiny používateľov jedna z verzií Windows. [28]



Obrázok 8 PCI karta - Ovislink AirLive WT-2000PCI

Ďalší typ kariet, sú karty typu PCMCIA, ktoré sú určené pre použitie v prenosných zariadeniach ako sú notebooky či PDA. Sú zhruba veľkosti kreditnej karty a veľa nových notebookov má WLAN kartu zabudovanú priamo na základnej doske.

Wi-Fi USB adaptéry sú veľmi lacnou alternatívou a sú do počítača zapájané pomocou USB kábla. Ich nevýhodou je to, že pracujú v systémoch Windows 98 a vyšších, takže v starších systémoch funkcie týchto adaptérov nevyužijú. Nespornou výhodou je ich veľkosť.

MiniPci sú karty ktoré sú na trhu len krátko, ale našli veľké uplatnenie pre Wi-Fi, používajú sa v súčasnosti skoro vo všetkých systémoch určených na sieťové operácie, hlavne ako prístupové body, ale dokážu pracovať aj ako klientské adaptéry, pre rôzne pásma od 700MHz až po 5GHz.

Z technického hľadiska sú lepšie hardwarové access pointy AP aj keď sú samozrejme drahšie. Umožňujú napojenie aj iných užívateľov a zdieľať ostatné pripojenia k internetu. K PC sa pripájajú cez metalické siete a obsahujú konektor na pripojenie antény. Obsahujú tiež niekoľko RJ45 portov a preto dokážu plniť funkciu mostu medzi PC na linke a PC napojenými cez Wi-Fi.

Medzi najrozšírenejšie zariadenia v súčasnosti patria Router platformy RouterBOARD. Sú to vlastne hardwarové dosky, ktoré obsahujú niekoľko ethernetových portov, niektoré už majú vstavanú pamäť s nahratým operačným systémom a veľmi výkonné sieťové procesory ktoré zvládajú náročné operácie. RouterBoard, ktorí chceme použiť patrí medzi najpredávanejšie platformy so vstavanou pamäťou a nahratým operačným systémom OS Mikrotik. Toto nie je jediné zariadenie na tejto platforme.

K pasívnym WiFi prvkom sieťové antény. Existuje niekoľko druhov v závislosti od použitia. Rozlišujeme či ide o anténu pre hlavný spoj, vysielanie pre klientov, alebo anténa ktorá je určená klientom. K hlavným parametrom uhol vyžarovania, zisk v dB a PSV čo je pomer stojatých vln. Existujú najčastejšie smerové antény, sektorové, satelity, vše smerové, Yagi, alebo aj iné neštandardné.

Ďalej patria k pasívnym prvkom pri stavbe WiFi siete káble, ktoré sú dôležité pre spojenie externej antény a Wi-Fi adaptéru. Je to kábel a vyrábajú sa v rôznych priemeroch a z rôznych materiálov. Rozhodujúcim prvkom je materiál, z ktorého je vyrobené jadro kábla a opletenie.

Ak používame kábel, je treba aj vhodný konektor a nahodenie konektorov nie je jednoduché preto sa to poručuje prenechať špecializovanej firme. Na trhu sa vyskytujú konektory niekoľkých typov a preto je vždy potrebné zistiť dopredu, aké sú potrebné. Najpoužívanejším je N – konektor a je vhodný aj na vonkajšie prostredie a hodí sa na montáž káblov až do hrúbky 4 -11mm. Ďalším často používaným konektorom je typ RSMA ale často vyskytuje aj konektor TNC.

1.7 Narušenie bezpečnosti WiFi komunikácie.

Bezdrôtové siete majú oproti káblovej sieti jednu veľkú nevýhodu, ktorá je spôsobená samotným princípom Wifi a to, že sa nedá obmedziť priestor, kde sa dá zachytiť signál WiFi siete. Signál sa šíri všetkými smermi a môže ho zachytiť ktokoľvek.

Z počítačov pripojených cez WiFi sa preto dá pomerne jednoduchým spôsobom zachytávať heslá a ďalšie dáta ak nie je prenos šifrovaný, zabezpečený. Vo WiFi sieťach je preto potrebné chrániť dáta, služby prenosu, spracovanie dát aj samotné zariadenia.

Vývojom technológií boli postupne prijímané rôzne opatrenia, aby sa siete stali bezpečnejšími. A dnes sa dá zabezpečenie rozdeliť do dvoch skupín podľa spôsobu a autorizáciu sme v predchádzajúcich kapitolách už popísali:

- Autorizácia – riadenie prístupu oprávnených užívateľov.
- Šifrovanie – zabezpečenie prenášaných dát pred odpočúvaním.

Bezpečnosť WiFi sietí môžeme rozdeliť podľa jednotlivých vrstiev. Na fyzickej vrstve ju riešime moduláciou, pretože pri prieniku musí útočník použiť rovnakú moduláciu ako sme použili my. Ak chce útočník preniknúť do siete musí tiež poznať sieťový identifikátor.

Tiež je dobré mať vyhradený priestor, kde bude WiFi signál šírený, aby sme mohli obmedziť prieniky signálu, čo je možné pomocou rôznych materiálov a použitím vhodných antén a ich smerovaním.

Bezpečnosť na spojovej vrstve je zabezpečované kódovaním informácií a prepájaním medzi mostmi VLAN, čo sú funkcie vrstvy a funkciami pod vrstvy MAC a to je manažment zahltenia siete, riadenie chýb, agregácia paketov alebo šifrovanie.

WiFi zariadenia majú na tejto vrstve funkciu filtrácie prístupu, zabezpečenú pomocou fyzických adries MAC cez ACL, Access Control List. Tento zoznam definuje pravidlá prí-

stupu, to znamená pre ktoré MAC adresy zo zoznamu je vysielanie povolené. Ďalším spôsobom v prípade prevádzkovania viacerých sieťových protokolov je filtrácia.

Bezpečnosť na sieťovej vrstve nie je normou špecifikovaná ale plní sa cez funkciu smerovania a podpory QoS. Filtrácia IP adres je potom riadenie prístupu na základe zoznamu autorizovaných IP adres a firewall sú bezdrôtové smerovače, ktoré môžu podporovať funkciu tak, že blokujú prenos z Internetu do Wi-Fi siete.

Bezpečnosť samotného prístupového bodu AP bude pre nás jedným z najdôležitejších bodov zabezpečenia. Budeme musieť zaistiť zabezpečenie neoprávneného prístupu a v prípade, ak by sa útočník predsa len na ňu dostal, aby nemal prístup ku kľúčom protokolov a nemohol by takto meniť ich nastavenia.

Existuje viac spôsobov, ale jedným z najspoľahlivejších a preto ho aj mi v praktickej časti použijeme, pretože máme tú možnosť je zakázať správu siete bezdrôtovo. Naše zariadenie toto nastavenie podporuje. Toto opatrenie spôsobí, že meniť nastavenia AP môžu iba tí, ktorí budú mať LAN prístup, kde je zariadenie pripojené.

Okrem toho aj po takomto opatrení musí byť samotné zariadenie ešte mechanicky chránené nie len z dôvodu, aby sa útočník nedostal k LAN, a nemohol ho resetovať. Bezpečnosť zvýšime tiež tým že preferujeme že naše zariadenie má pamäť flash, čo zjednodušuje implementáciu bezpečnostných záplat. V rámci bezpečnosti ešte odfiltrujeme užívateľskú prevádzku od správy siete.

II. PRAKTICKÁ ČASŤ

2 SPÔSOBY OPTIMALIZÁCIE WIFI SIETE

Po voľbe pre nás najlepšej metódy autentizácie a autorizácie a vykonaní všetkých potrebných opatrení, ktoré sa dajú vykonať nastavením vybraných zariadení je nutné zdefinovať prostredie s ohľadom na:

- požadovanú úroveň zabezpečenia,
- plochu ktorú bude treba pokryť,
- finančné prostriedky ktoré môžeme použiť,
- kompatibilitu sieťových adaptérov a operačných systémov.

Hlavným problémom pri vyberaní správnej metódy pripojenia a zabezpečenia býva aj, že na WiFi sa pripájajú užívatelia z rôznych sieťových adaptérov a s rôznymi operačnými systémami. Tento problém najlepšie rieši autentizácia pomocou metódy Hotspot Gateway, ktorá po autentizácii potrebujeme iba webový prehliadač. [29]

Pri použití iných metód, ktoré sú síce bezpečnejšie, ako autentizácia šifrovaním napríklad s autorizačným serverom pomocou osobných certifikátov, práve vzniká problém s kompatibilitou s rôznymi operačnými systémami a aj vysoká finančná náročnosť pri použití bezpečnejšej technológie.

2.1.1 Stanovenie požiadaviek na sieť

Sieťový hardware zahŕňa všetky technické prostriedky nutné pre fungovanie siete, ktorý sme čiastočne už popísali. Jedná sa o samotné pracovné stanice a servery, sieťové karty a adaptéry, huby čiže rozbočovače, switche čiže prepínače, routre čiže smerovače, repeátory čiže opakovače, bridge čiže sieťové mosty, gateway čiže brány a WAP čiže bezdrôtové prístupové body.

Súčasťou sú aj smerovacie protokoly, ktoré riešia usporiadanie týchto hardwarových zariadení. Na základe smerovacích protokolov pre ad-hoc wireless mesh siete, musia smerovacie protokoly čo najvernejšie spĺňať ďalej popísané požiadavky.

Prvou a najdôležitejšou požiadavkou je schopnosť siete fungovať a v prípade zlyhania niektorého z uzlov tak aby mohli smerovacie protokoly opakovať výber inej prístupovej cesty. Toto je výhodou mash smerovačov ktoré sme si vybrali pre realizáciu, je to im vlastný spôsob rozdeľovania záťaže. Mash smerovače dokážu vybrať najspoľahlivejšiu cestu pre dáta.

Ďalšou dôležitou požiadavkou pri návrhu WiFi siete je škálovateľnosť. Mash smerovač zvládnu veľké množstvo uzlov, pretože v rámci jednej siete nezávisia na nijakom centrálnom riadiacom uzle a škálovateľnosť je podporená smerovacími protokolmi. Závažnou požiadavkou je požiadavka na kvalitu služby vzhľadom na obmedzenú kapacitu kanálu.

Prenos bude založený na reaktívnych smerovacích protokoloch, ktoré zabezpečujú dostupnosť a údržbu trasy. Zdrojový uzol hľadá cestu k cieľovému uzlu a začne proces zisťovania trasy a zároveň zariadenie vykonáva údržbu trasy vzhľadom na typologické zmeny. Proces hľadania je dokončený v momente keď sa nájde celá cesta. Nevýhodou reaktívnych protokolov je oneskorenie vznikajúce hľadaním cesty pred posielaním packetu.

Konkrétne ide o pokrytie priestorov celého areálu väčšej výrobnéj a distribučnej poľnohospodárskej firmy pôsobiacej na vidieku signálom, umožniť pripojiť sa všetkým staniciam a serverom do internetu prostredníctvom Wi-Fi, vytvorenie užívateľských účtov pre všetkých zamestnancov s obmedzenou šírkou pásma 3072/3072 kbit/s. Využiť už existujúcu IT infraštruktúru.

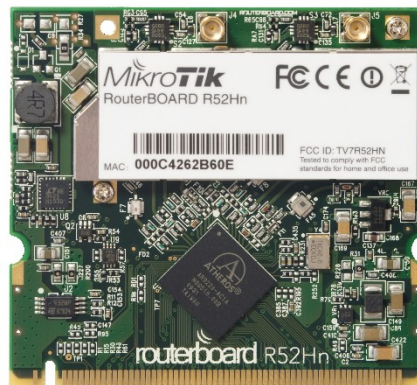
2.2 Komponenty siete

Medzi základné aktívne komponenty ktoré použijeme patrí RouterBOARD RB750 od výrobcu Mikrotik a ktorý má integrovaný RADIUS server, nakoľko ponúkajú užívateľsky jednoduché prihlásenie do siete bez nutnosti inštalácie ďalšieho softvéru, alebo certifikátov a z pohľadu ceny je to cenovo prijateľná platforma.

Router má v sebe tiež integrovaný HotSpot systém, ktorý sme spomínali a RADIUS obsahujúci RADIUS User Manager, ktorý slúži na prehľadnú správu. Zákazník potrebuje len webový prehliadač, kde zadá len prihlasovacie meno a heslo.

Bezdrôtová sieť sa skladá z týchto základných komponentov:

- Distribučný systém



Obrázok 9 802.11 Mikrotik

RouterBOARD RB750 Mikrotik je v podstate doska plošných spojov, zariadenie do ktorého sa vkladajú karty podľa zvoleného pásma, ktoré má niekoľko funkcií a je schopné pracovať v oboch frekvenčných pásmach a zastane aj funkciu routera. My vložíme kartu určenú pre pásmo 5 GHz typu R52Hn

Pri voľbe vyhovujúceho HW a SW riešenia pre realizáciu siete sme zvažovali použiť hardware od firmy CISCO, ktoré patria v dnešnej dobe k tomu najlepšiemu na trhu, pretože poskytuje veľký rad produktov pre prenos dát, hlasu aj videa

Má širokú podporu so strany ostatných výrobcov, ale nevýhodou komponentov od CISCO je ich omnoho vyššia cena za realizáciu a pomerne náročná konfigurácia, preto sme sa nakoniec rozhodli pre značku Mikrotik, ktorej výhody a možnosti dobre poznáme. Ďalším dôvodom tohoto riešenia je cena zariadenia, ktorá sa pohybuje okolo 30 - 100 €.

Výhodou je aj to, ako sme už spomínali, že Mikrotik Router má v sebe integrovaný systém HotSpot brány a podporu RADIUS servera, ktorého operačný systém sa dá nainštalovať na počítače architektúry x86, alebo využijeme RouterBOARD, čo je vlastne hardvérová platforma vyvíjaná spoločnosťou MikroTik.

Spoločnosť Mikrotik začala vlastný hardvér vyrábať v roku 2002 a jej routery sú dostupné v širokej škále od malých bezdrôtových klientskych jednotiek, až po vysoko výkonné centralizované smerovače. Výber závisí od ich úlohy a spôsobu nasadenia.

Nakoľko podmienkou realizácie bolo využiť aj existujúcu IT infraštruktúru, nebolo potrebné, aby HW mal bezdrôtové rozhrania čo tiež podporuje výber RouterBoard MikroTik RB750

Hardwarová konfigurácia a nastavenie pôvodného systému sú podobné, menia sa len podmienky Licencie operačného systému RouterOS, a to preto že sa zvýšil počet aktívnych užívateľov a počet PPPoE, L2TP, PPTP tunelov. Výrobok obsahuje HW časti aj operačný systém.

Technické parametre RouterBOARD RB750:

- RouterBOARD I RB750 - 5-portový ethernet router.
- RouterOS - Licencia L4.
- CPU: Atheros AR7240 400MHz .
- RAM:32 MB DDR SDRAM onboard memory.
- Teplotný pracovný rozsah:-40 °C až +55 °C.
- Operačný systém :MikroTik RouterOS v3
- Max Spotreba energie:2.5W.
- Rozmer:113x89x28mm
- Boot loader - RouterBOOT.
- Data storage 64MB onboard NAND memory chip.
- Architektúra: MIPS-BE.
- LAN porty: 5 x RJ45 10/100 Mbps MDI/MDI-X.
- PoE: 10-28V.

Je to z komponentov normy IEEE 802.11 a používa sa na presmerovanie dátového toku na stanicu určenia podľa aktuálnej polohy. Väčšina riešení je kombinácia bridge a distribučného média, použitého na prenos medzi dvoma prístupovými bodmi, najčastejšie sieťe intranetu.

- Bezdrôtové médium

Pri prenose dát je to nosič dát a pri prenose bezdrôtovo je to vzduch

- Stanica

Je akékoľvek zariadenie ktoré budeme mať pripojené do siete a bude komunikovať s prístupovým bodom pomocou sieťovej karty.

**Obrázok 10** Bezdrôtová sieť

- Prístupový bod

Access point AP je naše prekľutie medzi pevnou a bezdrôtovou sieťou, a zvykne obsahovať mnoho ďalších funkcií. Má rôzne použitia, ktoré sú podľa toho aké sú schopnosti tohto zariadenia. Pôvodne bolo WiFi navrhnuté ako bezdrôtové zariadenie pre lokálne siete a jej výhodou ako sme spomínali je práve to že využíva časť nelicencovaného pásma.

Dnes sa často používa práve pre pripojenie k internetu, pretože umožňuje budovať sieť LAN bez káblového pripojenie čo znižuje náklady a jednoducho umožňuje rozširovať bezdrôtové siete aj na neprístupné miesta.

Ako sme už spomínali pracuje v pásme 2,4 a 5 GHz a umožňuje zariadeniu, ktoré má bezdrôtové rozhranie a je v blízkosti prístupového bodu pripojiť sa k internetu. Signál pokrýva určité geografické územie a každý prístupový bod určitú oblasť.

Tento prístupový bod je aj Hotspot a niekoľko týchto bodov medzi sebou tvorí bezdrôtovú sieť a typická Wifi obsahuje niekoľko Hotspotov a každý Hotspot vysiela svoje sieťové meno SSID, Service Set Identifier. Každý klient ktorý sa pripojí na Hotspot komunikuje minimálne rýchlosťou 1Mbit/s. Pravidlá ochrany je hovoria, že niekoľko prístupových bodov a sieťových adaptérov, podporuje určitý stupeň kryptovania.

2.3 Implementácia WiFi siete

Vzhľadom k tomu, že sme sa rozhodli implementovať túto sieť pre výrobnú a distribučnú firmu, ktorej sídlo je na veľkej ploche, v zastavanej vidieckej oblasti prichádzajú do úvahy tri spôsoby sieťového pripojenia.

- Pripojenie káblovým rozvodom (optickým),
- Pripojenie k frekvenčnému pásnu 2,4 GHz,
- Pripojenie k frekvenčnému pásnu 5 GHz.

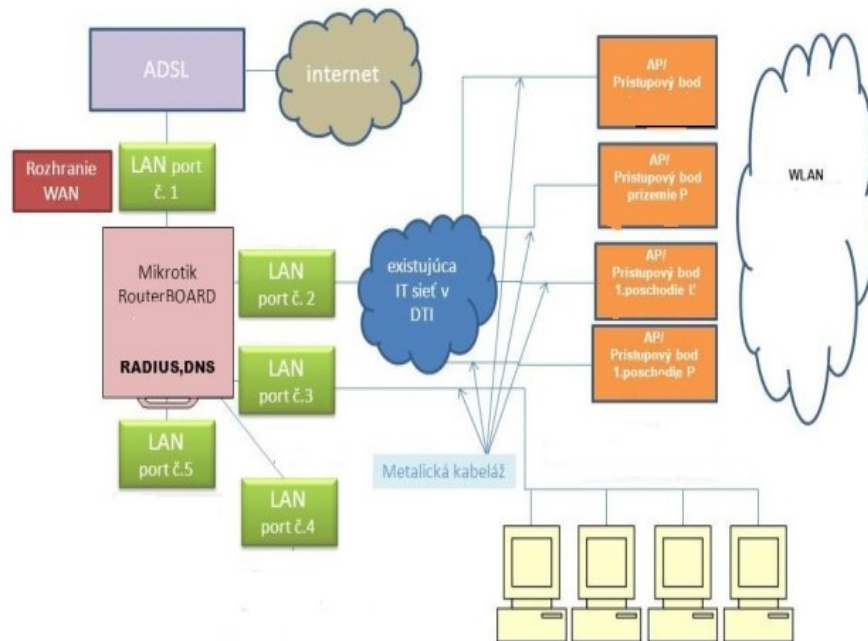
Budeme sa rozhodovať medzi pripojením k frekvenčnému pásmu 2,4 GHz a 5GHz. Prepojenie káblovým rozvodom vylúčime, okrem prepojenia AP. Konečné rozhodnutie urobíme podľa toho do akej výšky a s akým výkonom sa nám podarí umiestniť v areáli podniku vysielač. Pre túto stavbu bude sa jednať o budovu sila (zariadenie na úschovu suchých sypkých látok) ktorá je v tomto výrobnom podniku najvyššia. Zriadime tu, ak použijeme pásmo 2,4 GHz Nanostation 2 ak použijeme pásmo 5 GHz, Nanostation5.



Obrázok 11 Poľnohospodársky dvor s výškovou budovou v popredí

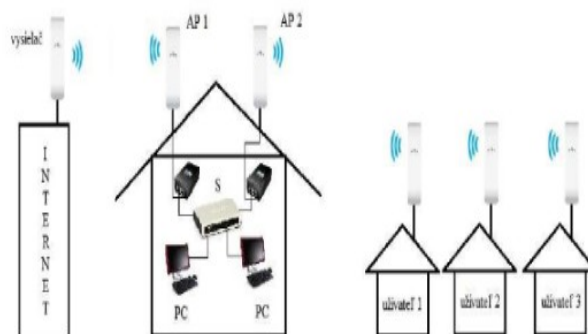
Zabezpečíme prijímacie a vysielačie zariadenie AP, ktoré umiestnime na tejto budove. Prijímač AP príma signál z iného vysielača a vysielač AP šíri tento signál ďalej. Na toto použijeme AP1, ktorý nastavíme ako prijímač a v softvéri ho nastavíme ako Client. AP2 nastavíme ako vysielač a v softvérovom rozhraní bude figurovať ako Access Point. Urobíme ich prepojenie cez priradený switch.

Z AP1 vyvedieme ethernetové pripojenie do miestnosti, ktorú používame pre umiestnenie serverov a do PoE portu adaptéra, ktorý musí byť pripojený do elektrickej siete a LAN konektor tohto adaptéra spojíme so switchom. Z AP2 tiež vyvedieme pripojenie do PoE adaptéra a konektor LAN spojíme so switchom. Vysielač AP2 ako sme už spomenuli vysiela SSID identifikátor na ktorý sa užívateľ vie pripojiť. Pripája sa AP2 v režime Client.



Obrázok 12 Topológia siete s HotSpotom

Ak budeme chcieť použiť pre pripojenie pásmo 5 GHz, postup je rovnaký, len je potrebné použiť Nanostation5. Pripojenie v pásme 5 GHz sa javí po zhodnutí všetkých stránok ako globalne najlepšie, pretože je približne rovnako finančne náročné ako v pásme 2,4 GHz a nepomerne lacnejšie ako pripojenie optickým káblom ale oproti pripojeniu v pásme 2,4 GHz je stabilnejšie v tomto prostredí vzhľadom k spoľahlivosti.



Obrázok 13 Sieťové pripojenie HotSpotu

Pri výstavbe vysielača budeme spolupracovať s miestnym poskytovateľom internetových a komunikačných služieb. Hlavný server bude vo výškovej budove v areáli podniku, odkiaľ je ideálny výhľad na ostatné budovy. Počet používateľov je niekoľko desiatok pracovných staníc. Sieť musí zohľadňovať koľko používateľov bude využívať služby v sieti a akú kvalitu očakávajú.

Ak plánujeme pokryť signálom zložitejšie priestory a musíme zrealizovať viaceré smerové spojenie, musíme sieť dôkladne naplánovať čo vyžaduje matematické výpočty, alebo simulácie, aby sme teoreticky overili či je projekt realizovateľný a predísť tak rušeniu spoja čo nám ušetrí finančné prostriedky a čas. Pred samotným plánovaním pokrytia sieťou musíme definovať:

- Oblasť pokrytia

To znamená, že musíme presne zistiť, aká bude veľká oblasť, ktorú pokrývame a aké veľké je množstvo používateľov v jednotlivých častiach siete. Ak je v tejto oblasti iný poskytovateľ pripojenia je dobré dohodnúť sa na harmonizácii, aby nedochádzalo k vzájomnému rušeniu sietí.

Ak chceme pomocou WiFi súvislo pokrývať kancelárske priestory, je nutné zakresliť podrobný plán vrátane prekážok, ako steny ktoré utlmia signál. Do plánu je potrebné zahrnúť koľko používateľov bude v daných miestnostiach.



Obrázok 14 Rozloženie budov v areáli

- Priepustnosť siete

Tento parameter hovorí o tom aké sú požiadavky na prenosové rýchlosti v sieti. Závisí od toho, akú technológiu použijeme a budeme sa rozhodovať medzi 802.11b alebo 802.11g.

- Možnosti mobility

Od tejto siete sa vzhľadom k náplni práce vyžaduje plná mobilita používateľov a teda plynulý prechod od jednej stanice ku druhej. Ak nie je dostupné mobilné pripojenie je požadované minimálne nemobilné pripojenie, ktoré bolo ako pôvodné v areáli firmy a ostane aktívne.

- Podpora chrbticovej siete

Znamená akým spôsobom bude realizované pripojenie bezdrôtovej siete do chrbticovej siete.

Takíto plán sa musí v praxi overiť, vykonať Site Survey mapovanie miesta. K tomu sa používa aplikácia pre meranie kvality signálu rádiovkej siete za pomoci potrebnej techniky ktorá je však drahá a určená pre rozsiahle projekty a preverenie plánu má poskytnúť tieto vedomosti:

- Aké je skutočné pokrytie prístupových bodov a ich optimálne pozícia v sieti
- Aké bude konečné reálne množstvo prístupových bodov potrebných pre pokrytie oblasti
- Aká je skutočné prenosová rýchlosť a chybovosť v sieti
- Či je prenosová rýchlosť a kvalita pre používateľov dostatočná

Tieto merania vykoná firma s ktorou spolupracujeme.

Ďalej je nutné efektívne využívanie frekvenčného spektra to znamená, že navrhne frekvenčné kanály pre jednotlivé prístupové body AP. Naša sieť obsahuje niekoľko prístupových bodov AP a musíme nastaviť na nich správne rádiové frekvencie, aby dochádzalo čo najmenej k vzájomnému rušeniu.

Štandardu IEEE 802.11, má iba tri frekvenčné kanály, ktoré sa neprekrývajú a pre minimalizáciu rušenia medzi prístupovými bodmi AP je najjednoduchší spôsob ako zvoliť správnu kombináciu frekvenčných kanálov. Z doteraz zistených informácií o prostredí a firme predpokladáme, že vzhľadom k členitosti terénu a rozmanitosti pripojených poľnohospodárskych zariadení, meračov a senzorov bude nami navrhované riešenie a prínos tejto práce návrh pripojenia na frekvencii pásma 5 GHz.

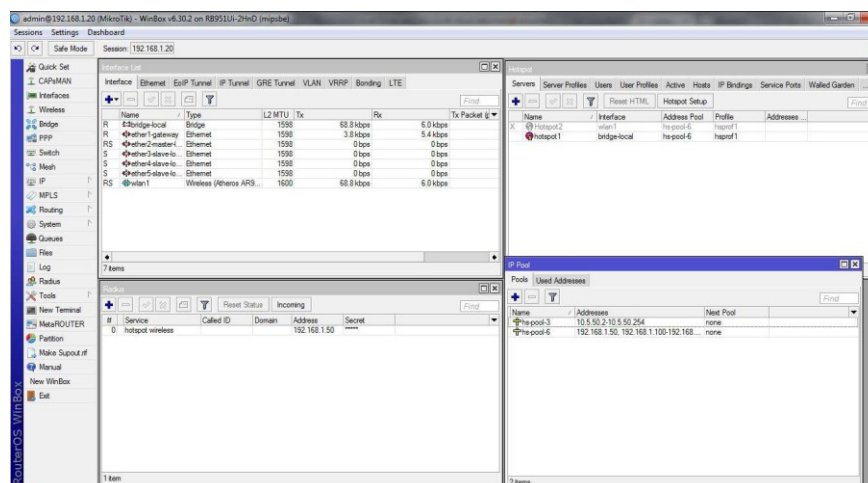
Ďalšie sieťové komponenty, ktoré využijeme by boli v jednom aj druhom riešení rovnaké a to bude parabolická anténa pre vysielanie - Rocket s externou sektorovou anténou a obe zariadenia budú pripojené na Mikrotik, ktorý je v podstate generátor siete. Mikrotik má

ako je naznačené na obrázku sériový port a tri LAN porty s rýchlosťou 100Mbit/s pre pripojenie počítača a jeden konektor RJ45. Port PoE je pripojený na LAN konektor a je určený na prenos elektrickej energie cez ethernet kábel.

Pre minimalizáciu rušenia využijeme zmenu smerovosti, alebo polarizácie vysielačích a prijímacích antén. Využijeme pokrývaný priestor a prístupový bod umiestnime ku stene s použitím sektorovej antény s vyžarovacím uhlom 180°. Takáto anténa nebude žiariť mimo nami požadovaný priestor. Pre spojenie bod – bod použijeme smerové antény s horizontálnou polarizáciou.

Ďalej použijeme HotSpot na platforme Mikrotik. Sieť môže mať rôznu veľkosť a to od jednoduchej malej siete s jedným aktívnym prvkom až po rozsiahlu sieť s niekoľkými desiatkami aktívnych prvkov. My budeme realizovať jednoduchšiu variantu s jedným aktívnym prvkom a HotSpot bude konfigurovaný na zariadení Mikrotik, ktorý nám bude poskytovať všetky funkcie pre nastavenie HotSpotu.

Zariadenie využíva RouterOS a RouterOS sa spravuje niekoľkými spôsobmi. Jedným je pripojenie cez linkovú vrstvu pomocou MAC adresy a využíva sa hlavne pri prvom spustení, keď nie je na zariadení nastavená žiadna IP adresa, alebo spôsob cez protokol TCP/IP, HTTP a pomocou sériovej linky. My budeme využívať spravovanie pomocou grafického rozhrania WinBox.



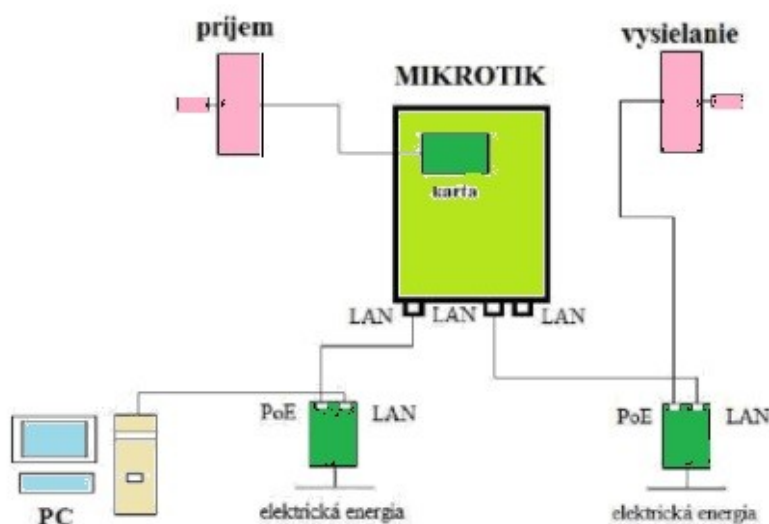
Obrázok 15 Aplikácia Win box

Winbox je najlepší nástroj, ktorým sa RouterOS spravuje. Je to MDI rozhranie, ktoré umožňuje ovládať a nastavovať všetky parametre RouterOS. Má prehľadné menu, cez ktoré sa dá jednoducho nájsť funkcia, ktorú hľadáme.

3 OPTIMALIZÁCIA WIFI KANÁLOV SIETE

Prvým krokom bude ako sme už spomínali vloženie karty pre pásmo 5GHz do zariadenia Mikrotik a pomocou obalu tohto plošného spoja zariadenie pevne umiestnime na konzolu. Následne pripojíme k zariadeniu parabolickú prijímaciu anténu, ktorá bude tiež na pevno.

Ďalším krokom je, že spojíme vysielaciu sektorovú anténu spojíme zo zariadením Nanostation M5 alebo s podobným zariadením, Rocket M5. Z tohto zariadenie ide ethernetový kábel do PoE adaptéra a následne do zariadenia Mikrotik. Do ďalšieho zariadenie pôjdeme cez napájací LAN port Mikrotiku a spojíme ho a ďalším PoE adaptérom



Obrázok 16 Schéma pripojenia vysielča

Po fyzickej výstavbe celej siete bude nasledovať softvérové nastavenie všetkých nastavení. Použijeme jeden z počítačov a pripojíme ho do LAN konektora v PoE adaptéri. Nainštalujeme spomínaný Winbox Loader.

3.1 Konfigurácia HotSpotov

Pre konfiguráciu HotSpot cez zariadenie Mikrotik RB využijeme päť konfigurovateľných portov, jedno bezdrôtové rozhranie pracujúce vo frekvenčnom pásme 5 GHz. Prístup do siete sme vybrali cez rozhranie ether1. Na tomto zariadení na ktorom máme internetové pripojenie už funguje DHCP server. Preto ether1 nastavíme na DHCP klienta.

To spôsobí že nám automaticky prideli IP adresu, masku siete, bránu a DNS server. Pre Mikrotik RB bola zvolená statická IP adresa a zapli sme funkciu NAT čo je prekladač IP adries z miestnej siete na verejnú IP adresu. Ostané porty ether2, ether3, ether4, ether5 a bezdrôtové rozhranie sme zapojili do jedného bridge.

Nastavenie RouterBOARD RB750

Nastavenie zrealizujeme cez WinBox, ktorý sme už spomenuli v predchádzajúcej kapitole, tak že sa prihlásime sa cez aplikáciu WinBox do vyresetovaného zariadenia ako admin bez hesla. Nastavenie robíme aj podľa topologickej mapy, ktorá nám vznikla meraním pomocou aplikácie Cleanair, ktorú opíšeme bližšie v neskoršom texte.

Kvôli prehľadnosti a neskoršej ľahšej administrácii si jednotlivé porty premenujeme. Prídáme IP adresy na rozhranie určíme adresu maska siete a broadcast adresa sa prepočíta automaticky. Ďalší krok je nastavenie DHCP klienta pre WAN a nastavenie DHCP servera pre LAN. V program sa zobrazí sprievodca pre nastavenie DHCP servera. DNS Server“ nakonfigurujeme na DNS-ISP.

3.2 Testovanie na reálnych zariadeniach a kompatibilita

Keďže vo firme existuje pôvodná sieť je potrebné posúdiť jej kompatibilitu so súčasnou sieťou. Ako sme už spomenuli pre prepojenie vonkajšieho a vnútorného zariadenia sme využili pôvodnú serverovňu. Tu bolo potrebné spojiť AP s kontrolerom ktorí sa nachádza v serverovni, použili sme pôvodnú štruktúru.

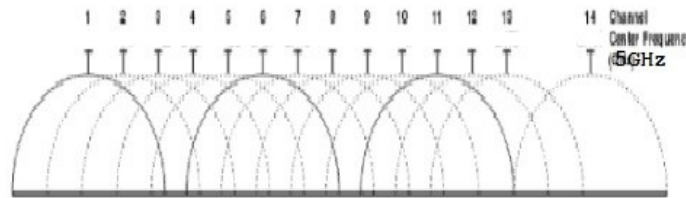
Nedostatok dostupných IP adries sme vyriešili teda pripojením kontrolera na smerovač Mikrotik, ktorý ako sme spomenuli zabezpečuje aj službu NAT. Vo vnútornej sieti používame IP adresy ktoré sa javia vďaka firewallu ako jedna IP adresa.

Je potrebné pri plánovaní zohľadniť prenosovú rýchlosť WLC kontrolera a prepínača a to tak že obe zariadenia musia podporovať rovnaké kapacity priepustnosti v sieti. Tiež je potrebné aby fungoval protokol pod ktorým komunikujú WLC a AP, my budeme využívať protokol CAPWAP.

3.3 Rozdelenie kanálov

Po umiestnení všetkých AP nasleduje testovanie. Aby sme zabránili malej priepustnosti musíme použiť dostatočný počet AP. Na druhej strane ak sa postavia tieto AP príliš husto

ich signáli sa miešajú. Samotné pásmo sa totiž dá rozkúskovať a nastaviť asi po 5 MHz nezávislých krokoch. Aj tak tieto frekvencie do seba zasahujú. Aby sa vysieláče nerušili nemôžu súbežne vysielat' všetky.



Obrázok 17 Rozdelenie pásma 2,4 GHz

Dnes už WCL dokáže automaticky v centralizovanej sieti analyzovať a merať rušenie v sieti a nastaviť tieto kanáli na vysielanie tak aby sa nerušili. Pásmo 5 GHz je citlivejšie ako pásmo 2,4GHz a preto použijeme technológiu DFS - Dynamic Frequency Selection, ktorá zabezpečuje že sú vždy vybrané pre zvolenú lokalitu najlepšie frekvencie.

WiFi router vysielá na určitej vybranej frekvencii. Týchto kanálov bolo v pásme 2,4 GHz určených 13 a na frekvencii 5 GHz a 19 na frekvenciách. Dnes sa vo veľkej väčšine používa skôr frekvencia 2,4 GHz. Jednoducho povedaná ak máme 13 dostupných kanálov, môže WiFi router komunikovať s 13 routami. Každý route bude mať svoj vlastný kanál.

Ale nie je to tak doslovne, tieto frekvencie musia mať medzi sebou nejaký malý odstup a router aj tak vysielaním na jednom kanáli presahuje aj do ďalších pásiem čím ostatné zariadenia v tomto pásme ruší. Veľkosť presahu závisí na tom aká je šírka kanálu, ktorú router ktorý použijeme využíva a to môže byť v pásme 2,4 GHz je 20 alebo 40 MHz.

Prakticky môžeme teda na 13 kanáloch v rozsahu 20 MHz umiestniť iba tri routery s takouto šírkou pásma, bez toho aby sa rušili. V kanáloch s rozpätím 40 MHz, môžeme použiť iba 2 route.

Vieme, že na obmedzený počet dostupných kanálov sa zmestí obmedzené množstvo routerov, bezdrôtových sietí a ak sa nenachádzame sa v hustej zástavbe napríklad na sídlisku, nemôžeme si dovoliť využiť frekvenciu 5GHz a zvýšiť tak koncentráciu bezdrôtových sietí a presahov spojených z rušením bez toho aby dochádzalo k vzájomnému rušeniu.

Rušenie sa v takejto sieti prejavuje tak, že klesá užitočný dosah a aj keď máte na zariadení viditeľný silný signál, internet ide zle, objavujú sa výpadky, rýchlosť kolíše. To je

v poslednom čase problém pásme 2,4 GHz a preto sme sa v našich podmienkach rozhodli využiť druhé pásmo.

Na zamedzenie rušenie je väčšina moderných prístrojov na frekvencii 5 GHz vybavená funkciou automatickej voľby kanála a router si automaticky vyberie najvhodnejší kanál a v prípade rušenia sa sám presunie na iný kanál.

Funkcia nám zabezpečí, že v prípade akéhokoľvek rušenia našej siete v poľnohospodárskom podniku sa bude mať signál kam sa premiestniť, pretože nepredpokladáme silné rušenie v celom pásme a teda ani časté striedanie kanálov čo by mohlo spôsobovať nestabilitu signálu.

Kanál nebudeme nastavovať na pevno a router sa nebude držať na danej frekvencii v prípade rušenia. Ako sme povedali rušenie sa častejšie vyskytuje v pásme 2,4 GHz, pretože je už preťažené a práve preto sme si zvolili ako riešenie takýchto problémov použitie nezrušeného 5GHz pásma.

Na frekvencii 5 GHz bude mať naša WiFi sieť k dispozícii rozsah 520 MHz a spolu 19 kanálov, ktoré sa navzájom neprekrývajú. Zatiaľ čo pri pásme 2,4 GHz je frekvenčný rozsah iba 82 MHz, u 5GHz je to vysokých 520 MHz, od 5,18 do 5,70 GHz.

Ako sme už spomenuli k dispozícii je tu celkom devätnásť kanálov s šírkou 20 MHz, ktoré sa už navzájom neprekrývajú. Tento fakt má ako dôsledok minimálne rušenie ostatnými zariadeniami a naozaj vysokorýchlostný prenos dát.

U 5GHz sietí však nie je všetko ideálne. Pokiaľ ho použijeme nastáva problém s menším dosahom signálu, ktorému robia prekážky väčší problém ako v prípade 2,4GHz siete. Pri šírke kanála 40 MHz môže v 5GHz pásme komunikovať súbežne deväť zariadení, bez toho aby sa navzájom rušili.

Vieme že nový štandardu 802.11ac má šírku kanála 80 MHz a fyzickú rýchlosť 433 Mb/s pre jeden stream, pri troch streamoch obsadíme polovicu 5GHz pásma.

Dnes je toto pásmo nedostatočne využívané ale v budúcnosti je možno očakávať, že aj 5GHz pásmo bude oveľa viac obsadené. A to z dôvodu že sa zvyšujú nielen požiadavky na rýchlosť, ale aj počet užívateľov, ktorí Wi-Fi používajú.

Rozšíriť pokrytie na terajších sieťach síce môžeme niekoľkými spôsobmi a tým najjednoduchším je ak vložíme do siete Wi-Fi universal repeater univerzálny opakovač. Ten urobí

to že prijme Wi-Fi signál a na rovnakom kanáli ho pošle ďalej a to preto že nemá dve rádiové rozhrania.

Frekvenční rozsahy kanálů ve 2,4GHz pásmu (2 401 až 2 483 MHz):

Pouze tři nepřesahující se 20MHz kanály (1, 6 a 11), celková šířka pásma jen 82 MHz

Kanál	1	2	3	4	5	6	7	8	9	10	11	12	13
Začátek	2 401	2 404	2 411	2 416	2 421	2 426	2 431	2 436	2 441	2 446	2 451	2 456	2 461
	MHz	MHz	MHz	MHz	MHz	MHz	MHz	MHz	MHz	MHz	MHz	MHz	MHz
Konec	2 423	2 428	2 433	2 438	2 443	2 448	2 453	2 458	2 463	2 468	2 473	2 478	2 483
	MHz	MHz	MHz	MHz	MHz	MHz	MHz	MHz	MHz	MHz	MHz	MHz	MHz

Obrázok 18 Frekvenčný rozsah kanálov v pásme 2,4 GHz

Ďalšou možnosťou je systém WDS, Wireless Distribution System ale jediným rozumným bezdrôtovým riešením WDS je použiť pre chrbticovej siete 5GHz pásmo, opäť ale narážame na problém, že musíte použiť veľa sieťových prvkov, routre musia byť v miestach silného signálu tých predchádzajúcich.

Frekvenční rozsahy kanálů v 5GHz pásmu (5 180 až 5 700 MHz):

Devatenáct nepřesahujících 20MHz kanálů, celková šířka pásma 520 MHz

Kanál	36	40	44	48	52	56	60	64	100	104	108	112	116
Frekvence	5 180	5 200	5 220	5 240	5 260	5 280	5 300	5 320	5 500	5 520	5 540	5 560	5 580
	MHz	MHz	MHz	MHz	MHz	MHz	MHz	MHz	MHz	MHz	MHz	MHz	MHz
Kanál	120	124	128	132	136	140							
Frekvence	5 600	5 620	5 640	5 660	5 680	5 700							
	MHz	MHz	MHz	MHz	MHz	MHz							

Obrázok 19 Frekvenčný rozsah kanákov v pásme 5 GHz

3.4 Cisco CleanAir

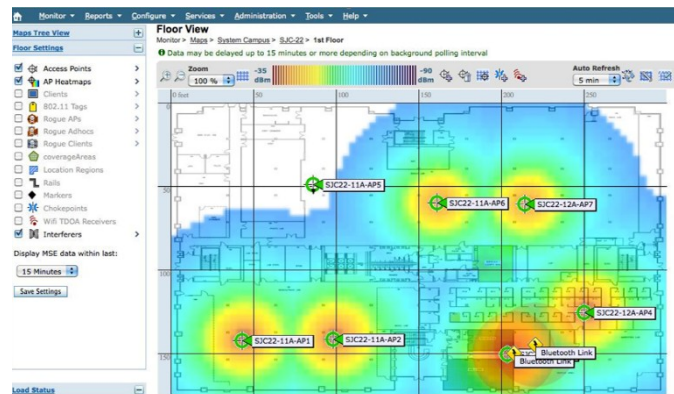
Ako sme už spomenuli, pokiaľ Wi-Fi nefunguje správne, môže to byť zapôsobené okolitými sieťami. Cisco CleanAir je technológia, ktorá využíva spektrálne analýzu. Obsahuje software a hardvér umožňujúci presne merať kvalitu WiFi kanálov a nájsť presne zdroje rušenia. Vyžaduje pre svoju prácu AP podporujúci Cisco CleanAir a Cisco WLAN kontroler.

Obsahuje Riadiaci systém WCS a Mobility service engine MSE čo sú dobrovoľné komponenty, ktoré výrobca dodáva pretože slúžia k získaniu kompletnej informácie o systéme, ktoré potrebujeme a to sú grafy, históriu, rušenie zariadení, lokalizačné služby a celkovú analýzu vplyvu. Jednotlivé AP potom zhromažďujú všetky informácie o zdrojoch rušenia. Spracuje ich a odovzdá koltroleru.



Obrázok 20 CleanAir Spectrum

Základom systému je CleanAir Spectrum Analysis Engine SAgE je to spektrálny analyzátor na čipe, ktorý má aj ďalšie funkcie. Toto zariadenie je extrémne presné a umožňuje nájsť rovnováhu medzi zariadeniami, pri veľkom množstve rušiacich zariadení a užívateľov.



Obrázok 21 CleanAir Spectrum graf

Toto zariadenie má technológiu umožňujúcu zistiť Index kvality ovzdušia AQI čo je univerzálna hodnota aký veľký je zásah rušenia do siete. Ak nie je prítomné žiadne rušenie hodnota je 100%. Hodnoty sú merané po sekundách, prepočítavané a posielané do regulátora. Všetko toto umožňuje aby kontroler prijal okamžité opatrenia na zaistenie problémov.

3.4.1 Identifikácia cudzích IP

Pomocou tohto zariadenia je možná aj identifikácia cudzích AP. Cudzíe zariadenia môžu zhustovať WiFi žiarenie a to bude mať nepriaznivý vplyv na našu sieť. Naše vlastné zariadenia sú pritom pod správou kontrolera, vedia o sebe a v prípade kolízie ich kontroler preradí na iné pásmo.

Nežiaduci signál nemá náš kontroler ako ovplyvniť, ale aspoň nás naše zariadenia upozorňujú na podstatu problému. V prípade že dochádza k pripojeniu používateľov našej siete mimo naše zariadenie dokáže AP odoslať takzvané authentication pakety, čo sa ale na týchto pásmach nepoužíva pretože je to nelicencované pásmo.

3.4.2 Roming

Pri centrálnom riadení je ďalšia dôležitá časť roaming klienta medzi jednotlivými AP. Postup je taký že sa skúšajúci s mobilným zariadením postupne prihlasuje medzi jednotlivými prístupovými bodmi AP a vyhodnocuje sa čas za aký sa pripojí zariadenie ak prejdeme do pôsobnosti iného AP. Tiež sa týmto spôsobom dá zistiť strata paketov v sieti. Roaming je možné nastaviť na ktorýkoľvek prístupový bod.

3.5 Další vývoj Wifi systémů

Ak sa s nadhľadom zamyslíme, nad problematikou WiFi zistíme že sa stala neoddeliteľnou súčasťou životov nás všetkých môžeme povedať, že si život bez nej nevieme vôbec predstaviť, určite by bol menej pohodlný a v niečom náročnejší.

WiFi vynášiel pán menom Vic Hayes ktorý pracoval pre spoločnosť NCR Corporation/AT&T v roku 1991. Už vtedy bola teoretická rýchlosť prenosu označovaného ako WaveLAN 1-2 Mbps, čo bol na ten čas nadštandard.

Široká verejnosť si WiFi vychutnala až v roku 1999 a vtedy bol predstavený aj štandard 802.11a, ktorý pracoval na 5 GHz frekvencii a neskôr bola pridaná podpora pre 3,7 GHz.

Prenos v pásme 5 GHz bol finančne náročný, a preto bol pomerne rýchlo vymenený za štandard 802.11b operujúci v pásme 2,4 GHz, čo bolo ideálnym riešením pri bezdrôtovom prenose na ďalších 5 rokov.

Nasledoval Bluetooth, ktorý bol obrovskou novinkou a ľuďom sľuboval vytvorenie aj vlastnej lokálnej siete v bezprostrednom okolí a naozaj rýchle vzájomné prepojenie niekoľkých zariadení. Táto technológia ako aj WiFi však na prenos využíva 2,4 GHz pásmo, ktoré sa časom začalo rýchlo plniť a vznikali rôzne nepríjemné interferencie.

Pribúdalo mnoho zariadení, ktoré sa pripájali k Wi-Fi, a tak nakoniec panuje v bezdrôtovom svete celkom slušný chaos. S Wi-Fi pripojením je to čoraz horšie pretože meste sa už už nenájdete byt, kde by nebol Wi-Fi router a do internetu pripájajú počítače, smartfóny, tablety, tlačiarne, televízory a mnohé ďalšie domáce spotrebiče.

95% ľudí však nevie, že Wi-Fi sieť môžu fungovať na rôznych kanáloch a tie treba, najmä v husto obývaných bytových domoch, využívať, aby bol signál Wi-Fi sietí čo najmenej rušený inou susednou Wi-Fi sieťou.

Ak si však aj dnes kúpime router s podporou vysielania štandardu Wi-Fi 802.11 ac, ktorý má problém so slabším signálom siete dokážeme ho už čiastočne odstrániť.

Po dvoch rokoch testovania Asociácia IEEE vydala a schválila Wi-Fi 802.11 ac, ktorá pracuje na 5 GHz frekvencii a ponúka niekoľko výhod voči štandardom fungujúcim na nižších frekvenciách ako je 2,4 MHz.

Okrem toho má 5 GHz frekvencia aj jeden vážnejší nedostatok. Tým je menší dosah a horšiu priechodnosť cez prekážky. V realite znamená že vo väčšom byte alebo dome budete

potrebovať viac routerov s podporou 5 GHz alebo je dobré ich skombinovať so zariadením, ktoré vysiela na 2,4 GHz.

Štandard Wi-Fi 802.11 ac ponúka údajne rýchlosť na úrovni 3,47 Gbps a zatiaľ nie je veľmi používaný. Štandard 802.11n pracujúci na frekvencii 2,4 GHz ponúka rýchlosť na maximálnej úrovni 600 Mbps.

Ako však stále opakujeme na tejto frekvencii je menej interferencií aj preto na 2,4 GHz dnes pracuje ešte stále väčšina Wi-Fi routerov, ale aj Bluetooth zariadenia a pásme 5 GHz je stále menej využívané aj napriek menšej náchylnosti na interferencie s inými Wi-Fi sieťami.

Čím menej šumu na prenášanej frekvencii vzniká, tým sú prenosové rýchlosti vyššie a prenos stabilnejší. Viac kanálov pre 5 GHz pásmo umožňuje routerom pracovať na viacerých pásmach ako v prípade 2,4 GHz sietí, čo znamená tiež menší šum a stabilnejší prenos.

Štandard Wi-Fi 802.11 ac ponúkajú aj lepší manažment a jednoduchšiu obsluhu. Väčšina používateľov stále nevie, ako si správne nastaviť svoju Wi-Fi sieť. V prípade štandardu 5 GHz je to aj pre menej zdatných používateľov jednoduchšie.

Množstvo routerov na tejto frekvencii totižto podporuje DFS, dynamickú voľbu frekvencie a to znamená, že si router sám vyberie, ktorý kanál je najmenej zahltený a ten bude používať tak ako sme to použili pri stavbe našej siete. DFS funguje priebežne, kanály si router dokáže prepínať a keď nájde vhodnejšiu frekvenciu na prenos s menším šumom prepne sa.

Výbornou vlastnosťou takto pokročilých routerov s podporou 5 GHz Wi-Fi siete je aj funkcia TPC Transmitting Power Control, ktorá automaticky reguluje energiu vysielajúceho signálu a automaticky reguluje žiarenie. A to znamená že ak máte router priamo na stole, vysiela signál len s takou energiou, aká je potrebná na plnohodnotný prenos medzi ním a vaším počítačom a pritom zbytočne nežiari na okolité zariadenia.

Toto má význam hlavne v otázke znižovania šumu na iných sieťach, ale aj zo zdravotného hľadiska. Vysoká kvalita signálu na kratšie vzdialenosti je zachovaná, signál s vyššou frekvenciou kmitá rýchlejšie, a dokáže cez prekážky prejsť kratšiu cestu ako signál s nižšou frekvenciou. V každom prípade je signál na kratšie vzdialenosti pri 5 GHz kvalitnejší, rýchlejší a stabilnejší.

ZÁVER

V tejto diplomovej práci sme chceli vysvetliť a názorne prezentovať, že zrealizovať bezpečnú a hlavne funkčnú sieť sa dá jednoduchým, a zároveň aj finančne nenáročným spôsobom. V prvej kapitole sme v teoretickej časti poukázali na rozdelenie sietí podľa rôznych kritérií a vysvetlili sme používané technológie v moderných WiFi sieťach.

V ďalšej kapitole sme rozobrali a načrtli hlavné dostupné metódy autentifikácie a spôsoby autorizácie užívateľov v bezdrôtových sieťach. S aspektom na mieru zabezpečenia sme zistili že je ideálne použiť autentizačnej metódy podľa štandardu IEEE.

Rozobrali sme potreby pre vybudovanie počítačovej siete, a zistili sme že problémom je rozmanitosť osôb a typov sieťových zariadení, ktoré využívajú Wifi štandardy. Najvhodnejšia je tá technológia ktorá obsahuje integrované HotSpoty a overovanie pomocou integrovaného RADIUS serveru, ktorý ponúka užívateľsky jednoduché prihlásenie do siete bez nutnosti inštalácie dodatočného softvéru, alebo certifikátov u zákazníkov cez prístupov body. Zákazník potrebuje len webový prehliadač, kde zadá prihlasovacie meno a heslo.

Z výrobcov aktívnych bezdrôtových zariadení sme vybrali cenovo prijateľnú platformu RouterBOARD RB750 od výrobcu Mikrotik. Funkcie, ktoré umožňuje, sa vyrovnajú oveľa drahším zariadeniam. Ako sme spomínali router má v sebe integrovaný HotSpot systém, RADIUS a User Manager, ktorý slúži na prehľadnú správu a ľahkú konfiguráciu systému.

Po nakonfigurovaní zariadenia vždy nasleduje overenie realizácie a je vykonávané pomocou rôznych diagnostických systémov, ktoré bez problémov identifikujú rôzne typy presahovania kanálov aj pokiaľ ide o susedné zariadenie. Centrálna správa a administrácia pomáha spresniť bezpečnostnú politiku siete.

Integrovaný firewall ponúka množstvo zaujímavých funkcií a základnou funkciou je detailné sledovanie prevádzky a samostatné reagovanie systému na rôzne stavy siete podľa nami určených pravidiel. Pomocou databázy v User Manageri si môžeme urobiť prehľad o každej činnosti užívateľa.

Klientom môžeme zariadenie Mikrotik len odporúčať pretože je to je to malé a výkonné AP, ktoré ma pre zákazníka aj správcu siete, mnoho výhod, a veľa problémov môžeme vyriešiť jednoducho a rýchlo.

5 GHz Wi-Fi sieť je niečo, čo vidí ako budúcnosť každý podporovateľ techniky a rýchleho pripojenia. Okrem vyšších rýchlostí a lepšej stability ponúka štandard aj ako sme spome-

nuli jednoduchšiu správu a nastavenia, pričom väčšinu dôležitých vlastností si sieť nastaví sama.

Už menšou výhodou je menší dosah a cena čo pri väčšom priestore vyžaduje na najlepšie pokrytie použiť viac routerov. Moderné routre dokážu vysielat' naraz Wi-Fi v režime 802.11 ac aj 802.11 n, takže v blízkosti routera môžete využívať rýchly 5 GHz internet a vo väčšej vzdialenosti stále solídnu Wi-Fi na 2,4 GHz.

Kombinácia týchto zmien viedla k rýchlejšiemu prístupu k údajom s rýchlejšiu odozvu pri načítaní stránok a pri súčasnom prístupe viacerých klientov. S veľkou pravdepodobnosťou môžeme predpokladať, že náš návrh je veľmi dobrým základom pre správu a overovanie aj väčšej siete do budúcnosti vybraného podniku.

ZOZNAM POUŽITEJ LITERATÚRY

- [1] ÚRAD PRE REGULÁCIU ELEKTRONICKÝCH KOMUNIKÁCIÍ A POŠTOVÝCH SLUŽIEB: Všeobecné povolenia [online]. [cit. 2017-05-23]. Dostupné z: www.teleoff.gov.sk/index.php?ID=29
- [2] BIGELOW, Stephen J. 2004 *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů*. Brno: Computer Press, 2004. ISBN 80-251-0178-9.
- [3] HORÁK, Jaroslav a Milan KERŠLÁGER. 2003., *Počítačové sítě pro začínající správce*. 3., aktualiz. vyd. Brno: Computer Press, 2006. Bestseller (Computer Press). ISBN 80-251-0892-9.
- [4] HORÁK, Jaroslav a Milan KERŠLÁGER. 2003., *Počítačové sítě pro začínající správce*. 3., aktualiz. vyd. Brno: Computer Press, 2006. Bestseller (Computer Press). ISBN 80-251-0892-9.
- [5] AKYILDIZ, Ian Fuat. a X. WANG. 2009., *Wireless mesh networks*. Chichester, U.K.: Wiley, 2009. ISBN 04-700-3256-1.
- [6] KÁLLAY, Fedor a Peter PENIAK. *Počítačové sítě a jejich aplikace: LAN / MAN / WAN*. 2. aktualiz. vyd. Praha: Grada, 2003. ISBN 80-247-0545-1.
- [7] *Mobilné rádiové siete*. Žilina: Žilinská univerzita, 2002. ISBN 80-710-0936-9.
- [8] CNEWS. *Technologie Bluetooth: bezpečnější a rychlejší: Rerakce Extranetobook*, [online]. 2017 [cit. 2017-05-08]. Dostupné z: <https://www.cnews.cz/hardware/>
- [9] SOS ELEKTRONIC. *Zigbee moduly na bezdrôtový prenos dát* [online]. [cit. 2017-05-08]. Dostupné z: <https://www.sos.sk/articles/no-name/zigbee-moduly-na-bezdrotovy-prenos-dat-543>
- [10] FLICKENGER, Rob. *Building wireless community networks*. 2nd ed. Sebastopol: O'Reilly, c2003. ISBN 05-960-0502-4.
- [11] NFC. *History of Mobile & Contactless Payment Systems* [online]. [cit. 2017-05-23]. Dostupné z: <http://nearfieldcommunication.org/payment-systems.html>
- [12] M-BUS CENTRÁLA. *Centrála pre M-Bus siete: katalóg* [online]. 2017 [cit. 2017-05-08]. Dostupné z: http://www.idamer.sk/ls_1110_sk_mbuscentrala_001.pdf

- [13] NATIONAL KNX. *Softwarové nástroje KNX* [online]. [cit. 2017-05-23]. Dostupné z: <https://www.knx.org/cz/knx/asociace/co-je-knx/index.php>
- [14] SOS ELEKTRONIC. *IQRF - bezdrátová technologie, která láme bariéry* [online]. [cit. 2017-05-23]. Dostupné z: <https://www.soselectronic.cz/articles/iqrf/iqrf-iqrf-bezdratova-technologie-ktera-lame-bariery-1342>
- [15] IRGF. *IQRF technology: Technology for wireless* [online]. 2017 [cit. 2017-05-08]. Dostupné z: <http://www.iqrf.org/technology>
- [16] PIŠKO, Michal. 2013., *Dostupnosť internetu u nás prudko rastie* [online]. [cit. 2017-05-23]. Dostupné z: <https://domov.sme.sk/c/7045140/dostupnost-internetu-u-nas-prudko-rastie.html#ixzz4hRRV2h84>
- [17] SANJINEZ, Mary Doly. 2013 *CLASIFICACIÓN DE LAS REDES ATENDIENDO EL TAMAÑO* [online]. [cit. 2017-05-23]. Dostupné z: <http://redesinformaticasmd.blogspot.sk/>
- [18] ZANDL, Patrick. 2003., *Bezdrátové sítě WiFi: praktický průvodce*. Brno: Computer Press, 2003. ISBN 80-722-6632-2.
- [19] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. Brno: CP Books, 2005. Cisco systems. ISBN 80-251-0417-6.
- [20] NAKHJIRI, Madjid. a Mahsa. NAKHJIRI. 2015., *AAA and network security for mobile access: radius, diameter, EAP, PKI and IP mobility*. Hoboken, NJ: John Wiley, c2005. ISBN 978-0-470-01194-2.
- [21] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. Brno: CP Books, 2005. Cisco systems. ISBN 80-251-0417-6.
- [22] LOVEČEK, Tomáš. 2007., *Bezpečnostné systémy: bezpečnosť informačných systémov*. Žilina: Žilinská univerzita v Žiline, 2007. ISBN 978-80-8070-767-5.
- [23] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. Brno: CP Books, 2005. Cisco systems. ISBN 80-251-0417-6.
- [24] LOVEČEK, Tomáš. 2007., *Bezpečnostné systémy: bezpečnosť informačných systémov*. Žilina: Žilinská univerzita v Žiline, 2007. ISBN 978-80-8070-767-5.
- [25] MINOLI, Daniel. 2003., *Hotspot networks: Wi-Fi for public access locations*. New York: McGraw-Hill, c2003. ISBN 00-714-0978-5.

- [26] MINOLI, Daniel. 2003., *Hotspot networks: Wi-Fi for public access locations*. New York: McGraw-Hill, c2003. ISBN 00-714-0978-5.
- [27] MINOLI, Daniel. 2003., *Hotspot networks: Wi-Fi for public access locations*. New York: McGraw-Hill, c2003. ISBN 00-714-0978-5.
- [28] ŽELEZNÝ, Petr. Bezdrátová technologie Wi-Fi. *The Standard for Wi-Fi* [online]. 2004 [cit. 2017-5-19].
- [29] McClure, Scambray, Kurtz. 2010. *Hacking bez záhad*. Praha : Grada Publishing 2007. 24-73 s. ISBN 978-80-247-1502-5.

ZOZNAM POUŽITÝCH SYMBOLOU A SKRATIEK

ISM	Industrial scientific and medical
IEE	Institute of Electrical and Electronics Engineer
WPAN	Wireless Personal Area Networks
ISM	Industrial, Scientific and Medical
CSMA/CD	Carrier Sense with Multiple Access and Collision Detection
ARCNET	Attached Resource Computer
WAN	Wide area network
EIB	European Installation Bus.
AMR	Systémy
AMI	Advanced Metering Infrastructure
EHSP	European Home System Protocol,
PAN	Personal Area Network
IrDA	Infra komunikácií
AES	Advance encryption Standard
NFC	Near Field Communication
WiFi	Wireless Fidelity
WECA	Wireless Ethernet Compatibility Alliance
IBSS	Independent Basic Service
AP	Aess point
SIG	Special Interest Group.
UDP	User Datagram Protocol
DNS	Domain Name System
PAP	Password Authentication Protocol
MD5	Message Digest Algorithm

ACL	Access Control List
SSID	Service Set Identifier
WDS	Wireless Distribution System
WCL	Wireless client

ZOZNAM OBRÁZKOU

Obrázok 1 Možnosti zapojenie siete WLAN, Pconfig.sk.....	16
Obrázok 2 JY-MCU Bluetooth Wireless Serial	17
Obrázok 3 iBMS systém SmartStruxure, sbs.sk.....	19
Obrázok 4 Rozdelenie sietí podľa veľkosti	24
Obrázok 5 Zapojenie PC klient - server	25
Obrázok 6 Zapojenie PC Peer-to-peer	25
Obrázok 7 Topológia sietí	26
Obrázok 8 PCI karta - Ovislink AirLive WT-2000PCI.....	33
Obrázok 9 802.11 Mikrotik	40
Obrázok 10 Bezdrôtová sieť.....	42
Obrázok 11 Poľnohospodársky dvor s výškovou budovou v popredí.....	43
Obrázok 12 Topológia siete s HotSpotom.....	44
Obrázok 13 Sieťové pripojenie HotSpotu	44
Obrázok 14 Rozloženie budov v areáli	45
Obrázok 15 Aplikácia Win box.....	47
Obrázok 16 Schéma pripojenia vysieláča.....	48
Obrázok 17 Rozdelenie pásma 2,4 GHz.....	50
Obrázok 18 Frekvenčný rozsah kanálov v pásme 2,4 GHz.....	52
Obrázok 19 Frekvenčný rozsah kanálov v pásme 5 GHz.....	52
Obrázok 20 CleanAir Spectrum	53
Obrázok 21 CleanAir Spectrum graf.....	54

ZOZNAM TABULIEK

Tabuľka 1 ISM pásma	14
Tabuľka 2 Porovnanie niektorých bezdrôtových pripojení ISM.....	15

ZOZNAM PRÍLOH

PRÍLOHA P I: NÁZOV PRÍLOHY